VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA

KATEDRA EKONOMICKÉ ŽURNALISTIKY

Vliv počítačové kriminality na společnost

The impact of computer criminality on the society

Student: Bc. Kateřina Kopečková
Vedoucí diplomové práce: JUDr. Tomáš Hulva

Ostrava 2011

VŠB – Technická univerzita Ostrava
Ekonomická fakulta
Katedra ekonomické žurnalistiky

Zadání diplomové práce

Student: **Bc. Kateřina Kopečková**

Studijní program: N6202 Hospodářská politika a správa

Studijní obor: 6202T095 Ekonomika a právo v žurnalistice

Téma: Vliv počítačové kriminality na společnost
The impact of computer criminality on the society

Zásady pro vypracování:
1. Úvod
2. Příčiny vzniku a možnosti prevence počítačové kriminality
3. Ekonomické a právní důsledky počítačové kriminality
4. Ochrana dat
5. Závěr
Seznam použité literatury
Seznam zkratek
Prohlášení o využití výsledků diplomové práce
Přílohy

Seznam doporučené odborné literatury:

MATĚJKA, M. *Počítačová kriminalita*. 1. Vyd. Praha: Computer Press, 2002. 106 s. ISBN 80-7226-419-2.
GŘIVNA, T.; POLČÁK, R. *Kyberkriminalita a právo*. 1. Vyd. Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.
DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* 1. Vyd. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **JUDr. Tomáš Hulva**

Datum zadání: 26.11.2010

Datum odevzdání: 29.04.2011

_____	_____
doc. PhDr. PaedDr. Milan Sekanina, CSc.	prof. Dr. Ing. Dana Dluhošová
vedoucí katedry	*děkanka fakulty*

"Místopřísežně prohlašuji, že jsem celou práci vypracovala samostatně a uvedla jsem všechny použité zdroje."

Ostrava 29. dubna 2011

…….

Podpis

Obsah

1 Úvod

S informačními technologiemi se v dnešní době střetáváme na každém kroku. Jejich přínos ve všech oblastech výroby, obchodu, směny, komunikace či zábavy je naprosto neoddiskutovatelný. Bohužel, průnik těchto doposud málo známých a ve své podstatě velmi složitých technologií do všech oblastí běžného života s sebou nutně musí nést i své stinné stránky. Jednou z nich je právě počítačová kriminalita, fenomén, který se objevil s nástupem „digitálního věku“. Zvláštnosti tohoto druhu kriminality vyplývají již ze samotné podstaty moderních informačních technologií.

Nové technologie totiž umožňují potencionálním pachatelům páchat velmi propracovanou a předem promyšlenou trestnou činnost pomocí výpočetní techniky, konkrétně tedy pomocí počítačů, které jsou připojené k síti Internet. Tyto kriminální delikty se vyznačují téměř dokonalou anonymitou a mohou probíhat na zcela libovolně velkou vzdálenost. Tímto způsobem lze páchat obrovskou škálu trestných činů, které mají v důsledku velmi negativní ekonomický dopad na různé subjekty.

V první části mé diplomové práce se zaměřuji na charakteristiku pojmu *„počítačová kriminalita“*. Věnuji se zde jejím historickým aspektům s ohledem na vývoj výpočetní techniky a informačních technologií. Nezbytnou součástí obecné terminologie je také definování profilu pachatele počítačové kriminality a jeho motivace k protiprávnímu jednání. Za velmi důležitý prvek teoretické části považuji zaměření na možnosti prevence a represe s ohledem na tento druh kriminality. Je zřejmé, že jakákoliv represe by nemohla být účinná bez odpovídajícího stupně prevence a naopak.

V hlavní části mé práce se věnuji tematickému rozřazení nejvýznamnějších projevů počítačové kriminality a jejich ekonomických a právních dopadů na společnost. Pro kompletní přehled legislativní úpravy doplňuji veškerá protiprávní jednání příslušnými paragrafy a zákony. Uvádím také fakta o kybernetických hrozbách a informační bezpečnosti v České republice ve srovnání se zahraničním prostředím.

V závěrečné kapitole se zabývám ochranou dat s důrazem na porušování autorských práv a ochranu osobních údajů a na právní úpravu dané problematiky.

Hlavním cílem mé diplomové práce je podat čtenáři ucelený pohled na problematiku počítačové kriminality, její nejdůležitější aspekty a její právní a ekonomický dopad na společnost. Z důvodu nadnárodní rozsáhlosti kybernetických hrozeb, se zaměřuji také na mezinárodní aktivity spojené s preventivními opatřeními, včetně zapojení České republiky do

těchto projektů. Snažím se také poukázat na ne zcela dokonalou právní úpravu stále se vyvíjejícího druhu kriminální činnosti a na hrozby, které z ní vyplývají.

2 Příčiny vzniku a možnosti prevence počítačové kriminality

2.1 Vymezení pojmu počítačová kriminalita

Počítačová kriminalita je mladý, přesto dynamicky se rozvíjející obor. Má řadu výrazných charakteristik, které ji odlišují od kriminality klasické. Ve většině případů se neobjevují takové prvky, jako je násilí, použití zbraně, újma na zdraví osob apod. Zatímco u klasické kriminality se měří doba spáchání trestného činu na minuty, hodiny a dny, trestný čin v oblasti počítačové kriminality může být spáchán v několika tisícinách vteřiny a pachatel ani nemusí být přímo na místě činu. Významnou charakteristikou pro počítačovou kriminalitu jsou v jejím důsledku značné ztráty, ať již přímo v podobě finančních částek, nebo v podobě zneužití získaných údajů. Počítačovou kriminalitu také provází určitá diskrétnost trestné činnosti. Pachatel musí být zpravidla vyzbrojen hlubšími předmětnými i technickými znalostmi z oblasti informačních technologií, zejména počítačů. Z uvedeného vyplývá, proč počítačová kriminalita bývá pro svou povahu někdy označována též jako kriminalita „bílých límečků“.[1]

Mezi běžně používané názvy pro tuto problematiku patří *počítačová kriminalita*, *kriminalita informačních technologií* a *kyberkriminalita*.[2] Nesnadnost vymezení počítačové kriminality je příčinou velké variability přístupů k vyjasnění a chápání tohoto pojmu. Počítačovou kriminalitu lze definovat nejobecněji jako každou nekalou činnost páchanou s pomocí počítačů. Pojem „nekalá činnost“ může být specifikována např. společenskou nebezpečností důsledků, které tato aktivita přináší. Což přichází v úvahu zejména v případech přestupků, trestných činů či obecně deliktů ve smyslu porušení platné zákonné úpravy. Aby bylo možno hovořit o počítačové kriminalitě, musí pachatel ke svému jednání užít nejen výpočetní techniku, ale jeho jednání musí také naplňovat znaky skutkové podstaty některého trestného činu uvedeného v trestním zákoníku a nebezpečnost takového jednání musí dosahovat požadovaného stupně nebezpečnosti činu pro společnost.

Za počítačovou kriminalitu lze považovat trestné činy, jejichž objektem, eventuálně objektivní stránkou bude informační technologie v plném slova smyslu. Jedno z možných členění počítačové kriminality přijala Rada Evropy. Jejím smyslem je mimo jiné sjednotit

[1] MUSIL, S. Počítačová kriminalita: Nástin problematiky. Praha, 2000, s. 12.
[2] MATĚJKA, M. Počítačová kriminalita. Praha, 2002, s. 3.

legislativu Evropských zemí, nejen proto, že se jedná o problematiku počítačové kriminality, ale také z toho důvodu, že tato trestná činnost má mezinárodní charakter.[3]

Rada Evropy přijala členění počítačové kriminality ve formě[4]

- *minimálního seznamu aktivit:*

  - Počítačové podvody, včetně nedovolené manipulace,
  - Počítačová falzifikace, stíhaná podobně jako falzifikace tištěných dokumentů,
  - Poškozování počítačových dat,
  - Počítačová sabotáž, včetně útoků proti hardwarovým prostředkům,
  - Neoprávněný přístup,
  - Neoprávněný průnik, včetně neoprávněného používání komunikačních sítí počítačů a přístupu k datům jejich prostřednictvím,
  - Neoprávněné kopírování autorsky chráněného programu,
  - Neoprávněné topografie, včetně ochrany čipů,

- *volitelného seznamu aktivit:*

  - Změna v datech nebo počítačových programech ve významu změn především bez finančního profitu, kdy však může dojít k dalekosáhlým následkům, např. při zpracování osobních dat,
  - Počítačová špionáž, především zneužíváním průmyslového a obchodního tajemství,
  - Neoprávněné užívání autorsky chráněného programu.

Rozsah problematiky počítačové kriminality velmi dobře dokumentuje také preambule Manuálu pro prevenci a kontrolu počítačového zločinu OSN.[5]

[3] POŽÁR, J. Některé trendy informační války, počítačové kriminality a kyberterorismu. Dostupný z http://www.svses.cz/skola/akce/konf/bezp05/texty/pozar.pdf.
[4] Úmluva Rady Evropy o počítačové kriminalitě, Budapešť, 23. listopadu 2001, Convention on Cybercrime - ETS no. 185.
[5] Manuál OSN pro prevenci a kontrolu počítačového zločinu, OSN 1994.

„Rozvoj světa informačních technologií s sebou nese i stinné stránky (...). Počítačové systémy nabízejí nové a vysoce sofistikované možnosti porušování práva a především potenciálu pro páchání tradičních typů zločinů netradiční cestou. K ekonomickým škodám, které počítačová kriminalita přináší, je třeba připočíst závislost celého lidstva na počítačových systémech doslova ve všech oblastech denního života, od řízení letecké, železniční i autobusové dopravy po zdravotnictví a obranu. I malá chyba v počítačovém systému může znamenat ohrožení lidských životů.“

Všechny definice se v zásadě shodují v tom, že je nutné rozlišit dvě základní kategorie počítačové kriminality. Jednou z nich jsou protiprávní jednání směřující proti počítači, kdy je počítač přímo terčem útoku. Jedná se především o průniky do systémů za účelem krádeže dat, průmyslové špionáže, bankovního podvodu, zneužití osobních údajů z elektronické databáze apod. Další jsou protiprávní jednání spáchaná s využitím počítačů.

S tímto jednoduchým rozdělením není možné vystačit. Počítačovou kriminalitu je také nutno rozdělit z jiného hlediska. Může jít:[6]

- O protiprávní jednání tradiční, kde počítač pouze usnadňuje jejich spáchání, ať už je přímo jejich terčem nebo jejich nástrojem.
- O protiprávní jednání zcela nová, která se objevila až s nástupem moderních informačních technologií, ať už směřující proti počítači, či používající počítač v roli nástroje.

2.1.1 Úmluva o počítačové kriminalitě

Převratný vývoj výpočetní techniky ovlivňuje všechny stránky lidského života. Na jedné straně usnadňuje a racionalizuje nesčetnou řadu lidských činností, na druhou stranu integrace telekomunikačních a informačních systémů skýtá možnosti pro páchání trestné činnosti. Připojením na komunikační a informační služby vytváří jednotliví uživatelé určitý druh společného prostoru, který lze nazvat „kyberprostorem“. Zároveň tak vzniká jako nechtěný produkt určitý prostor pro společensky nebezpečné aktivity nového typu. Kriminalita páchaná v kybernetickém prostoru se vyznačuje řadou specifik. Kyberprostor nezná hranic. Kriminální

[6] MATĚJKA, M. Počítačová kriminalita. Praha, 2002, s. 6.

útoky v kyberprostoru jsou velmi efektivní. Umožňují z jednoho místa zasáhnout chráněné zájmy na mnoha jiných místech ve velmi krátkém čase, v podstatě se zanedbatelnými finančními náklady a s minimálním nebezpečím okamžitého odhalení. Zatímco kybernetický prostor je prostorově neomezený, normy trestního práva platí jen na území příslušného státu. Z toho rozporu plyne výhoda pro pachatele využívající k páchání činů kyberprostor. Má-li se společnost efektivně bránit, je nezbytná určitá míra harmonizace trestněprávních norem (hmotných i procesních) a usnadnění mezinárodní spolupráce mezi státy v potírání společensky škodlivých jevů v kybernetickém prostoru. Jedním z nástrojů k dosažení nastíněného cíle je právě Úmluva.[7]

Úmluva je výsledkem čtyřleté práce expertů Rady Evropy, USA, Kanady, Japonska a dalších. O sestavení komise expertů v oblasti počítačové kriminality bylo rozhodnuto již v listopadu 1996 Evropským výborem pro otázky kriminality, který vycházel ze zprávy vypracované na její žádost prof. Kaspersenem, jenž na závěr doporučil, aby došlo k harmonizaci právních úprav na základě právního instrumentu s větším dosahem, než je Doporučení.[8] Předmětem úpravy by mělo být nejen trestní právo hmotné, ale též právo procesní a rovněž pravidla mezinárodní spolupráce.

Výčet pojmů používaných opakovaně v Úmluvě, týkající se počítačové kriminality:[9]

„Počítačovým systémem“ se rozumí jakékoli zařízení nebo skupina vzájemně propojených nebo souvisejících zařízení, z nichž jedno nebo více provádí na základě programu automatické zpracování dat. Podle Úmluvy je tedy počítačovým systémem zařízení sestávající se z technického (hardware) a programového (software) vybavení, které je určené k automatickému zpracování bez přímého lidského zásahu. Zpracování dat znamená, že na data se v počítačovém systému působí prostřednictvím počítačového programu.

„Počítačovými daty“ se rozumí jakékoli vyjádření skutečností, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému včetně programu vhodného k zajištění, aby počítačový systém vykonával určitou funkci.

Dalším pojmem jsou *„nosiče informací“* (dat), jimiž se rozumí snadno přenosná média, která slouží jako prostředek k záznamu dat, přičemž je pojem *„nosič informací“*

[7] GŘIVNA, T.; POLČÁK, R. Kyberkriminalita a právo. Praha, 2008, s. 104.
[8] Doporučení č. R (89) 9, týkající se trestního práva hmotného a Doporučení č. R (95) 13, týkající se trestního práva procesního.
[9] GŘIVNA, T.; POLČÁK, R. Kyberkriminalita a právo. Praha, 2008, s. 106.

totožný s pojmem *„nosič dat“*.[10] Pod tyto nosiče můžeme podřadit jak jednotky do počítače pevně zabudované (operační paměti nebo pevné disky) tak přenosné (diskety, paměťové karty či výměnné disky).

Úmluva o počítačové kriminalitě obsahuje znaky devíti trestných činů, které dělí do čtyř kategorií. Mimo to se Úmluva týká některých otázek základů trestní odpovědnosti (účastenství, pokus trestného činu, odpovědnost právnických osob) a sankcí. Při vymezení znaků jednotlivých činů, jejichž kriminalizaci Úmluva vyžaduje, je téměř vždy uveden výslovně znak protiprávnosti slovy „neoprávněně“, „protiprávně“. Tím má být zdůrazněno, že mohou existovat i činnosti dovolené, i když vykazují všechny další znaky uvedených činů. Typickými případy, kdy je vyloučena protiprávnost, jsou např. činnosti přikázané nebo dovolené právním řádem, jednání v nutné obraně a v krajní nouzi, souhlas poškozeného apod. Ani jeden trestný čin definován v Úmluvě nelze spáchat z nedbalosti. Objektem těchto trestných činu je ochrana důvěrnosti, neporušenosti a použitelnosti počítačových systémů nebo dat, ochrana před sexuálním zneužíváním dětí, ochrana literární, umělecké a vědecké tvůrčí činnosti a jejich výsledků. Pokud jde o trestné činy související s počítači, individuálním objektem je ochrana počítačových dat, údajů a systémů, pokud jde o jejich důvěrnost. Změna dat, údajů a systémů bývá většinou prostředkem pro spáchání jiných trestných činů.

Úmluva stanoví znaky těchto trestných činů:[11]

- Trestné činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů
  - Neoprávněný přístup
  - Zásah do dat
  - Zásah do systému
  - Zneužití zařízení
- Trestné činy související s počítači
  - Falšování údajů související s počítači
  - Podvod související s počítači
- Trestné činy související s obsahem
  - Trestné činy související s dětskou pornografií

[10] SMEJKAL, V. Počítačové právo. Praha: C.H. BECK, 1995, str. 103.
[11] Úmluva o počítačové kriminalitě. Budapešť, 23.11.2001. Dostupné z http://translate.google.cz/translate?hl=cs&langpair=en|cs&u=http://en.wikipedia.org/wiki/Convention_on_Cybercrime.

- Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu

Neoprávněný přístup

Objektem tohoto činu je ochrana před ohrožením bezpečnosti počítačových systémů a dat. Potřeba ochrany odráží zájem korporací a jednotlivců řídit, provozovat a kontrolovat své systémy nenarušovaným způsobem a bez zábran. Objektivní stránka spočívá v přístupu do počítačového systému nebo jeho části. O neoprávněný přístup se jedná, když dojde k porušení bezpečnostních opatření, úmyslu získat počítačová data nebo jinému nečestnému úmyslu, nebo je čin proveden ve vztahu k počítačovému systému, který je propojen s jiným počítačovým systémem.

Neoprávněné zachycení informací

Objektem neoprávněného zachycení informací je ochrana práva na soukromí datové komunikace. Tento čin lze ve své podstatě přirovnat k tradičním odposlechům, vztahuje se na veškeré formy přenosu elektronických dat. Objektivní stránka činu spočívá v zachycení neveřejných přenosů počítačových dat pomocí technických prostředků, a to z počítačového systému nebo v rámci něj. Smluvní státy mohou prostřednictvím kvalifikačních okolností omezit trestnost na případy nečestného úmyslu, nebo je-li čin proveden ve vztahu k počítačovému systému, který je propojen s jiným počítačovým systémem.

Zásah do dat

Objektem tohoto činu je ochrana počítačových dat a počítačových programů před úmyslným způsobením škody – porušením integrity, nesprávným fungováním nebo neoprávněným využíváním uložených počítačových dat nebo počítačových programů. Objektivní stránka spočívá v poškození, vymazání, zhoršení kvality nebo změně počítačových dat. Je možné, aby si smluvní státy vymezily trestnost pouze na činy, které vedou ke vzniku závažné újmy.

Zásah do systému

Objektem činu je ochrana zájmu operátorů a uživatelů počítačových nebo telekomunikačních systémů na řádném fungování těchto systémů. Objektivní stránka spočívá v závažném narušení fungování počítačového systému vložením, přenesením, vymazáním, poškozením, zhoršením kvality, nebo změnou počítačových dat. Do této kategorie spadá také

odesílání dat určitému systému v takové podobě, objemu nebo frekvenci, že to má za následek škodlivý vliv na schopnost vlastníka využívat systém, nebo komunikovat s ostatními systémy.

Zneužití zařízení

Objektem tohoto činu je zájem na ochraně společnosti a osob před možným ohrožením vyplývajícím z nekontrolované výroby, prodeje, jiné distribuce a držení věcí, které primárně slouží k trestné činnosti v kybernetickém prostoru, nebo pomocí nichž lze získat přístup k počítačovému systému nebo jeho části. Ke spáchání trestného činu je často potřeba opatřit si některé z přístupových prostředků, jako jsou různé hackerské nástroje. Objektivní stránka spočívá:[12]

- ve výrobě, prodeji, obstarání k užívání, dovozu, distribuci nebo jiném zpřístupnění:
  - zařízení, včetně počítačového programu určeného primárně pro účely spáchání trestného činu,
  - počítačového hesla, přístupového kódu nebo podobného údaje, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části;
- v držení jakékoliv výše uvedené věci.

Všechny smluvní státy si mohou sami určit minimální počet takových věcí pro vznik trestní odpovědnosti.

Falšování údajů související s počítači

Objektem je ochrana důvěry ve spolehlivost elektronických dat, která mohou mít důsledky v právních vztazích. A objektivní stránka spočívá v jakékoliv změně počítačových dat, které vedou ke vzniku nepravdivých údajů. Jedná se o obdobu padělání hmotných dokumentů. V tomto případě není rozhodující, zda se jedná o data na veřejné či soukromé listině.

Podvod související s počítači

Objektem tohoto trestného činu je ochrana společnosti před nepatřičnou manipulací v průběhu zpracování dat se záměrem dosáhnout nezákonného převodu vlastnictví. Objektivní stránka spočívá ve způsobení ztráty jiné osobě a to především jakýmkoliv zásahem do

[12] GŘIVNA, T.; POLČÁK, R. Kyberkriminalita a právo. Praha, 2008, s. 116.

počítačového systému. Jednání musí být činěno s nečestným úmyslem získat protiprávně pro sebe nebo jinou osobu hospodářský přínos.

Trestné činy související s dětskou pornografií

Objektem činu je ochrana před sexuálním zneužívám dětí. Je zde uvedeno poskytnutí ochrany před chováním, které by mohlo vést k podněcování nebo svádění dětí ke skutečnému sexuálnímu zneužívání. Objektivní stránka spočívá:[13]

- ve výrobě dětské pornografie pro účely její distribuce prostřednictvím počítačového systému,
- v nabízení nebo zpřístupňování dětské pornografie prostřednictvím počítačového systému,
- v distribuci nebo přenášení dětské pornografie prostřednictvím počítačového systému,
- v obstarávání dětské pornografie prostřednictvím počítačového systému pro sebe nebo pro jinou osobu,
- v držení dětské pornografie v počítačovém systému nebo na médiu pro ukládání počítačových dat.

Zpřístupnění zahrnuje mimo jiné také tvorbu nebo kompilaci odkazů na stránky s dětskou pornografií. Všechny smluvní státy jsou oprávněny učinit výhradu, která se může týkat neuplatnění trestnosti při obstarávání dětské pornografie.

Trestné činy související s porušením autorského práva a práv příbuzných autorskému právu

Objektem tohoto činu je ochrana literární, umělecké a vědecké tvůrčí činnosti a jejich výsledků. Objektivní stránku tvoří jednání spočívající v porušení autorského práva tak, jak je definováno v právním řádu každého smluvního státu, jestliže však došlo k porušení pomocí počítačového systému.

2.2 Výpočetní technika a vývoj počítačové kriminality

Výpočetní technika zasahuje do stále většího počtu oblastí a svou dynamikou vývoje navozuje nové vztahy a problémy nebo mění jejich obsah. Jde o nový, dynamický fenomén ve společnosti, který se nutně odrazí v mnoha právních odvětvích. Znamená nejen očekávaný a

[13] GŘIVNA, T.; POLČÁK, R. Kyberkriminalita a právo. Praha, 2008, s. 119.

uznávaný přínos, ale přináší s sebou i nové a ne vždy pozitivní jevy a skutečnosti. Pojmy jako počítačová kriminalita, softwarové pirátství, ohrožení informací a následně pak počítačová bezpečnost, autorská práva, ochrana dat, ochrana soukromí atd., se však již dostávají i do povědomí širší veřejnosti. Růst podílu výpočetní techniky na zpracování informací všeho druhu je neoddělitelnou součástí rozvoje společnosti a je třeba ho chápat nejen jako samozřejmý technický vývoj, ale i jako proces sociální.[14] Vznik počítačové kriminality vyplývá z historického vývoje výpočetní techniky. Počátečním impulsem bylo masové využívání osobních počítačů a jejich propojování do sítí, a to především internetu. Vznik existence internetu znamenal zásadní zlom ve kvalitě, ale také ve kvantitě zločinů týkajících se počítačů. V České republice je vývoj docela odlišný oproti ostatním státům a to proto, že zavedení informačních technologií bylo opožděné. K prvním trestným činům v této oblasti dochází až na konci 80. let, kdy se v tehdejších československých domácnostech začaly objevovat první osobní počítače.[15]

První sálový počítač se jmenoval ENIAC. Byl sestrojen na Pensylvánské univerzitě v roce 1946. Tyto počítače byly využívány na přelomu 50. a 60. let v mnoha společnostech, ale také na univerzitách.[16] Údržba těchto strojů byla velmi finančně a časově náročná, proto docházelo k zásahům do programů, tzv. „hacks“, které měly zefektivnit chod operačního systému a různých aplikací. První generací hackerů byla v 60. letech identifikována skupina studentů, která měla k těmto počítačům přístup.

V 70. letech začalo zneužívání telefonních linek. Touto činností se zabývají tzv. phreakers. Rok 1971 navíc proslul případem Cap ´n´ Crunch. Právě tak se jmenovala značka cereálií, do nichž byla přidávána dětská píšťalka. Veterán vietnamské války John Draper objevil, že právě tato píšťalka vydává zvuk o frekvenci 2600 HZ, který při použití v telefonní lince dovolí uskutečňovat hovory zdarma. Roku 1975 S. Wozniak a S. Jobs (zakladatelé firmy Apple Computers) začali vyrábět tzv. „blue boxes“, zařízení založené na Draperově objevu. Na konci 70. let došlo k důležité události. Byl sestrojen první BBS (Bulletin Board Systém), díky němuž se uživatelé, kteří vlastnili počítač s telefonní linkou, mohli stát součástí kyberprostoru. K rozšíření těchto technologií došlo až s představením osobních počítačů firmou IBM, které s sebou přinesly jednoduchý operační systém a masovou výměnu dat a programů mezi uživateli.[17]

[14] MUSIL, S. Počítačová kriminalita. Praha, 2000. Dostupné z http://www.ok.cz/iksp/docs/256.pdf.
[15] PAUKERTOVÁ, V. Elektronická informační kriminalita. 2006. Dostupné z http://www.ikaros.cz/node/3554.
[16] ENIAC. Dostupné z http://cs.wikipedia.org/wiki/ENIAC.
[17] MATĚJKA, M. Počítačová kriminalita. Praha, 2002, s. 21.

K rozšíření předchůdce dnešního internetu (BBS) došlo v 80. letech díky počítačům IBM, které byly čím dál více propojovány do sítí. Většinou se jednalo o servery s textovým rozhraním, na které se připojovalo přímou volbou čísla. Z tohoto fenoménu vzešla skupina hackerů „Legion of Doom“, která nebyla organizovaným společenstvím osob, neměla stálé členy, hierarchii ani nic podobného. Jejich nepostradatelnou činností bylo publikování článků v undergroundových médiích. Na konci 80. let došlo k obrovskému rozšíření hackerských skupin.[18] V roce 1982 přichází na trh nové médium pro záznam digitálních dat CD-ROM, což vedlo ke kvalitativnímu zvýšení pirátských aktivit. V roce 1987 se na Delawarské univerzitě objevil *první virus*, který nezpůsobil žádné trvalé poškození, pouze drobné systémové chyby. Neodmyslitelnými osobnostmi tohoto desetiletí byl také vysokoškolský student z Cornellovy univerzity Robert Morris Jr., který poslal roku 1988 do světa svůj virus InternetWorm, a Kevin Mitnick, který je znám především svým útokem na počítače společnosti Digital Equipment. Téhož roku také došlo ke slavné počítačové krádeži v chicagské First National Bank, která tak přišla o 70 milionů dolarů.

V 90. letech dochází k masovému rozšíření osobních počítačů, zejména s operačním systémem MS Windows, čímž vzrůstá i vývoj příslušného softwaru. Důsledky v trestné činnosti nese náhlý rozvoj počítačových sítí a to především internetu. Internet se začíná dostávat z akademických kruhů do komerční sféry a stává se tak velmi lákavou a snadnou příležitostí k páchání nelegálních aktivit. Tím se v 90. letech začíná rozvíjet globální počítačová kriminalita. Z typického pachatele předchozích etap, tedy původně počítačového nadšence, se stává chladný profesionál, jehož cílem je vlastní obohacení. Na počátku 90. let dochází v České republice k obchodování s nelegálním hudebními a filmovými a také s nelegálním software. Podle BSA (Business Software Aliance) dosahovala míra používání nelegální software až 80 %. S nárůstem kupní síly obyvatelstva a šířenou osvětou o nelegálním používání software se začala situace pozvolna měnit. V roce 2004 klesla míra softwarového pirátství na 40 %. V České republice začíná docházet také ke zneužívání osobních dat, bankovním podvodům, internetovým podvodům a šíření pornografie. V roce 1996 se na českém a slovenském internetu objevuje hackerská skupina CzERT a Binary Division, která se specializuje na pozměňování webů.[19]

V současné době je naše společnost stále více závislá na počítačích a počítačových sítích. Počet uživatelů internetu den ode dne roste. Prudký rozvoj internetu změnil chápání autorského díla, internet se také stále více stává nástrojem organizovaného zločinu. Počítačoví

[18] MATĚJKA, M. Počítačová kriminalita. Praha, 2002, s. 22.
[19] PAUKERTOVÁ, V. Elektronická informační kriminalita. 2006. Dostupné z http://www.ikaros.cz/node/3554.

piráti se spojují do skupin a rychle se šíří nelegální software, objevují se padělky hudebních a filmových autorských děl. Čím dál častěji se objevují nové typy útoků, jako jsou spamming, phishing, pharming a rozesílání malware. Rozšiřují se typy útoků, při kterých dochází k heslování souborů uložených v počítači na dálku a následné výkupné na software. V roce 2000 hacker MafiaBoy napadl významné webové servery jako Yahoo či eBay a získal tak přístup k 75 počítačům v 52 sítích a spouštěl na nich různé aplikace. V témže roce byl objeven také vir „I love you“, který způsobil škodu asi 10 miliard dolarů. Jeho autorem byl filipínský student Onel DeGuzman, který vzhledem k neexistenci příslušné filipínské legislativy nemohl být odsouzen. V letech 2000 až 2001 probíhal soudní spor mezi internetovým portálem Yahoo a francouzskou ligou proti rasismu LICRA. LICRA žalovala Yahoo za propagaci nacismu, neboť přes aukční stránky portálu byly přístupné nacistické materiály. Roku 2002 byl zatčen Gary McKinnon z Velké Británie, který pronikl do více než 90 počítačů americké armády ve Velké Británii. V roce 2005 došlo k největšímu útoku na bezpečnost bankovních dat - kvůli nedostatečným směrnicím a nařízením společnosti MasterCard bylo ohroženo až 40 milionů kreditních karet. Tentýž rok se na internetu objevily nové verze virů. V modifikované variantě zaútočil několik let starý vir Sober, který je součástí e-mailu tvářícího se, že jeho odesílatelem je FBI.

V České republice dochází v roce 2000 asi k nejznámějšímu případu. Počítačová firma Mironet byla obviněna z instalace nelegálního software. Po neúspěšné policejní prohlídce případ utichl, Mironet však nakonec žaloval firmu Microsoft, která několik let vyvíjela tlak na instalace operačního systému Windows, a tak upadla v podezření z policejního udání. Mezi další případy můžeme zařadit umístění pirátských kopií českých filmů na internet, bankovní podvody, krádeže citlivých údajů a jejich následný prodej, či také e-mailové hrozby.[20]

2.3 Příčiny vzniku počítačové kriminality

Příčiny vzniku počítačové kriminality přímo vyplývají z historického vývoje. Například prapůvod průniku do systému je ve zcela legitimní snaze odstranit jeho chyby a optimalizovat ho pro co možná nejefektivnější využití. Až později, s masovým využitím počítačů, ale především s rozvojem jejich propojování do rozsáhlých sítí typu internet spolu se vzrůstající potřebou komerčních subjektů se k takovým sítím připojovat, začalo být pro pachatele

[20] PAUKERTOVÁ, V. Elektronická informační kriminalita. 2006. Dostupné z http://www.ikaros.cz/node/3554.

zajímavé, používat k nelegálním průnikům do systémů za účelem krádeže dat nebo elektronických loupeží na bankovních účtech počítače.

Literatura[21] většinou uvádí jako základní kriminogenní faktory, které mají vztah k počítačové kriminalitě, případně ji usnadňují následující:[22]

Složitost informačních technologií a jejich provozu je pro značnou část uživatelů neproniknutelná. Z toho pramení vnímání světa počítačů jako něčeho neuchopitelného a již od základu podezřelého.

Důvěra uživatelů ve výstupy z informačních technologií. Klasicky se zde uvádí skutečnost, že málokoho napadne kontrolovat například účet připravený počítačovým systémem v supermarketu, či ověřovat správnost výpočtů provedených počítačem v rámci firemního účetnictví. V důsledku toho může zůstat dlouho neodhalen pachatel počítačového podvodu či zpronevěry, který si z finančních toků procházejících systémem pravidelně odečítá mikroskopické částky pro vlastní obohacení apod.

Objem dat v prostředí, kde se pachatelé pohybují, je často enormní. Je technicky neproveditelné efektivně kontrolovat veškerá data procházející třeba internetem.

Páchání trestné činnosti *od obrazovky počítače* je neporovnatelně *snazší*, než je tomu v reálném životě.

Obecně *nízké právní vědomí* populace, které se projevuje i v jiných oblastech práva, je v případě informačních technologií ještě nižší. Tento stav je nicméně zcela pochopitelný a to jak z oblasti veřejného, tak soukromého práva. Normy, které se týkají oblasti informačních technologií, jsou často velmi složité.

Nedokonalost legislativy. Právní normy upravující oblast informačních technologií jsou mnohdy obtížně vyložitelné a jejich mezerovitost je značná. Vzhledem k dynamickému vývoji v této oblasti tomu jinak ani být nemůže, protože ucelená soustava právních norem se nemůže vytvořit, dokud nedojde ke konsolidaci dotyčného odvětví.

Informační a komunikační technologie mají mnoho vlastností, které nesou mnoho výhod jak pro bezúhonného běžného uživatele, tak pro zločince. Moderní technologie mají také nevýhodu pro specializované bezpečností složky. Umožňují globální dostupnost tak, že

[21] STERLING, B. Zátah na hackery - chaos a nepořádek v elektronickém pohraničí. 1992. Dostupné z http://knihovnicka.mysteria.cz/zatah.pdf.
[22] MATĚJKA, M. Počítačová kriminalita. Praha, 2002, s. 8.

vzdálenost mezi pachatelem a obětí není ničím omezena a tím je útočník schopen uskutečňovat trestnou činnost ze vzdáleného místa. Zajišťují značnou míru anonymity, přitom samotný obsah komunikace nemusí být nijak zvlášť důležitý, ve srovnání se zjištěním, kdo, kdy a s kým komunikoval. Také ceny výpočetní techniky neustále klesají a tím jsou mnohem dosažitelnější pro širší skupiny lidí a navíc ovládání výpočetní techniky nevyžaduje nijaké speciální či odborné vzdělání. Přenos dat prostřednictvím výpočetní techniky je velmi rychlý a to umožňuje kriminálním skupinám přenášet, kopírovat, pozměňovat a ničit velké objemy dat. Mezi útočníky a běžnými uživateli existuje značná asymetrie. Tím, kdo volí metodu, okamžik a cíl útoku, je vždy útočník. Je velmi obtížné se útoku bránit, neboť protiopatření, která by útok proti kybernetickým systémům odrazila, jsou obrovsky nákladná.[23]

2.3.1 Vznik počítačové kriminality v České republice

Páchání počítačové kriminality se v samých počátcích na našem území omezovalo na poměrně úzký okruh zaměstnanců výpočetních středisek, kteří měli jako jediní přístup k výpočetní technice. Teprve v osmdesátých letech se situace začala měnit a počítače se začaly vyrábět i u nás, do té doby se do domácností dostávaly jen velmi zřídka.

Jako první počítačový zločin u nás je uváděn případ pracovníka Úřadu důchodového zabezpečení v Praze, který mstíc se podniku a státnímu zřízení, nosil po dobu více jak jednoho roku v prostorách sálu s počítačem, v rozporu s provozními předpisy, dámské silonové prádlo, což způsobovalo elektrické výboje, které měly za následek poruchy počítače. Dále pak umísťoval magnetická media s daty do blízkosti silných zdrojů elektrického napětí nebo magnetů, které i sám přinášel. Touto činností ochromil provoz výpočetního střediska a zapříčinil pozastavení výplat důchodů v celé ČSR. Jeho jednání bylo podle tehdejší právní úpravy kvalifikováno podle § 97 TrZ jako sabotáž.[24]

Jako hlavní příčinu vzniku počítačové kriminality v České republice lze považovat ekonomickou transformaci po roce 1989, především tedy rozsáhlé společenské změny, jako je právní a morální vědomí společnosti. K dalším důvodům jistě patří také technický rozvoj, který usnadňuje páchání trestné činnosti a podmiňuje vznik nových forem deliktů. Zásadní vliv na vznik trestné činnosti u nás mají také legislativní změny. Zejména devadesátá léta minulého století byla poznamenána chaosem a nepřehledností v legislativě. Český právní řád

[23] JIROVSKÝ, V.; HNÍK, V.; KRULÍK, O. Kybernetické hrozby: výzva pro moderní společnost. 2008. Dostupný z http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/kyberneticke_hrozby.pdf.
[24] BÍMOVÁ, Alena. Počítačová kriminalita a naše doba. 1991, str. 81.

je velmi složitý, naplněný neustálými novelami, a proto je možné si stejné právní normy vyložit různými způsoby. Což v důsledku znamená, že třeba k daňovým únikům nemusí dojít přímo s úmyslem, ale díky nesprávné interpretaci příslušné právní normy. Počítačová kriminalita vzrůstala nejen proto, že se objevovaly stále nové a nové příležitosti k jejímu páchání, ale také vlivem ekonomické krize a neuvážených vládních reforem, díky čemuž se lidé dostávají do materiální nouze. Tuto situaci mohou uspokojit motivy, jako je např. vylepšení společenské prestiže, postup na společenském žebříčku a výrazné vylepšení materiální situace. Navíc většinou si pachatelé myslí, že jejich zaměstnání není dostatečně oceněno a mají pocit převahy nad zaměstnavatelem, pocit beztrestnosti a neodhalitelnosti. Je zřejmé, že kdyby pachatelé věnovali stejné úsilí legálním činnostem, mohli by být také úspěšní, ne-li úspěšnější.

2.4 Prevence a represe z pohledu počítačové kriminality

Prevence kriminality bývá v řadě prací naší i světové kriminologie definována různě. Podle jedné z nejkomplexnějších definicí, náleží do prevence kriminality veškeré aktivity, které směřují k předcházení páchání trestných činů, ke snížení jejich výskytu cestou zamezení páchání nebo neutralizací příčin a podmínek vzniku trestných činů. Patří sem opatření, jejichž cílem či důsledkem je zmenšování rozsahu a závažnosti kriminality prostřednictvím omezení kriminogenních příležitostí nebo působením na potencionální pachatele a oběti trestných činů. Prevence tedy představuje pokus o eliminaci trestné činnosti ještě před jejím započetím nebo před jejím pokračováním.[25]

Represi v oblasti počítačové kriminality provádí, tak jako u ostatních protiprávních činů, státní orgány – policie, soudy aj. Jejich úkolem je vyšetřování správních deliktů, přestupků a trestných činů a ukládání sankcí, které jsou stanoveny zákonem. Efektivní, v případě protiprávního jednání, je rychlá a závažnosti provinění úměrná sankce. Je zde ovšem patrný limit, na který represe v oblasti počítačové kriminality naráží. Represivní složky jsou velmi často o krok za pachateli. V důsledku toho je vypátrání pachatele a shromáždění důkazů o jeho protiprávním jednání často velmi obtížné. Policie sice zaznamenává nepřehlédnutelné úspěchy v boji proti pachatelům počítačové trestné činnosti, ale řádově mnohem více těchto skutků zůstává nepotrestáno. Příčinou je kromě obtížnosti vyšetřování těchto trestných činů také skutečnost, že oblast počítačů je stále zatížena nízkým právním vědomím veřejnosti.

[25] MUSIL, S. Počítačová kriminalita. 2000. str. 224.

Počítače samy o sobě jsou tak často vnímány jako velmi obtížně pochopitelná technologie, natož aby existovalo povědomí o právních normách platných v této oblasti. Práce represivních složek v oblasti počítačové kriminality je náročná, a to nejen technologicky, ale především znalostně. Ve vyspělých zemích proto vznikají speciální týmy pro boj s tímto typem zločinnosti, většinou na centrální úrovni, případně na nejvyšší úrovni jednotlivých územních celků. Tyto týmy mají za úkol cíleně bojovat proti počítačovému zločinu. Bývají mnohem lépe vybaveni než ostatní složky policie či státní správy a jejich základním předpokladem je neustálé vzdělávání v oblasti dané problematiky. I přesto jsou její možnosti omezeny. Nejenže na rozdíl od pachatelů musí dodržovat zákon, který v řadě případů v úmyslu chránit občany před nežádoucím vlivem státní moci do sféry soukromí jednotlivce vlastně neúměrně zatěžuje, tak také přímo znemožňuje efektivní vyšetřování obtížně objasnitelných zločinů, jako jsou ty počítačové. Úkol orgánů činných v trestním řízení, v tomto případě především policie, spočívá v tom, aby zajistily takové množství důkazního materiálu, aby mohl být obžalovaný nad veškerou pochybnost usvědčen a tedy shledán vinným a odsouzen. Bohužel ve virtuálním světě je právě tento požadavek klíčovým problémem dokazování počítačového zločinu. Orgány činné v trestním řízení musí vždy porušení zákona dokázat konkrétní osobě.[26]

V České republice se prevenci počítačové kriminality věnují mimo státních orgánů také různá zájmová sdružení a nevládní organizace. Jednou z nich je firma *„Business Software Alliance“*[27], která se zabývá především softwarovým pirátstvím. Pravidelně informuje uživatele internetu svými prohlášeními o pokročilých vyhledávacích metodách vedoucích k odhalení stále většího procenta protiprávně se chovajících a jednajících pachatelů. Dalším, v tomto případě již úzce zaměřeným sdružením, zabývajícím se ochranou, ale také prevencí před nelegálním kopírováním hudebních produktů je *„IFPI“*[28], sdružující na pětadvacet českých i nadnárodních firem. Obě výše zmíněné organizace bojují s počítačovou kriminalitou především v rámci prevence skrz různé kampaně či slogany, jejichž hlavním cílem je odrazení od páchání protiprávní činnosti.

Za velmi důležitý prvek prevence lze považovat také jistý stupeň počítačové gramotnosti mezi lidmi, kteří užívají výpočetní techniku. Znalost praktik, které používají pachatelé počítačové kriminality, ale také způsobů, jak je co nejvíce eliminovat nebo alespoň zmírnit, je další možnost, jak předcházet velkému množství útoků a jednání, která jsou protiprávní.

[26] MATĚJKA, M. Počítačová kriminalita. Praha, 2002, s. 81.
[27] Business Software Alliance. Dostupné z www.bsa.org.
[28] IFPI. Dostupné z www.ifpicr.cz.

Globální úroveň takového vědomí však není na dostatečně vysoké úrovni, tudíž není tato forma prevence zcela efektivní.

2.4.1 Obecné prostředky počítačové bezpečnosti

Všechny prostředky počítačové bezpečnosti nelze jednoznačně hodnotit podle jejich významnosti. Priority při jejich výběru je nutno podmínit konkrétními možnostmi např. podniku a ochotou vedení věnovat na tyto účely určité, často nemalé finanční částky. Podle toho lze hovořit o různých úrovních počítačové bezpečnosti. Vždy je však důležité, aby všechna opatření, nehledě na jejich úroveň, na sebe úzce navazovala a logicky se vzájemně doplňovala. Není možné, aby byla nahodile vybrána jen některá z nich, byť by se zdálo, že nejúčinnější, pokud bychom nerespektovali vazby na další podstatné aspekty. Opatření, která se na první pohled jeví jako nejúčinnější, mohou být účinná jen v adekvátním kontextu s jinými způsoby zvýšení počítačové bezpečnosti. Jinak samozřejmě mohou svou účinnost skutečně ztratit.

2.4.2 Projekty počítačové bezpečnosti

Každá instituce, která obhospodařuje citlivá data většího rozsahu, by měla ustanovit specialistu pro počítačovou bezpečnost. Jeho opodstatnění je evidentní zejména u podniků s velkou koncentrací výpočetní techniky, při práci ve větších sítích, často s nepřehlednými vazbami mezi jednotlivými účastníky, obsáhlých databázích či při časté manipulaci s daty početným kolektivem zaměstnanců. Tento pracovník by měl nejenom dohlížet nad realizací opatření zajišťujících počítačovou bezpečnost. Měl by navíc přistupovat k systému ochrany informací tvůrčím způsobem tak, aby byl schopen ji neustále zlepšovat a interaktivně reagovat na případné její nedostatky. K tomu je zpravidla nutno zpracovat určitý projekt počítačové bezpečnosti, který musí přihlížet ke všem hypotetickým variantám chování systému či potenciálních narušitelů. Komplexní systém ochrany by měl vycházet z vnitřního bezpečnostního standardu instituce. Měl by přihlížet k několika kriteriím, jako je typ informací, k typu komunikace s dalšími sítěmi, k objemu a frekvenci manipulací s daty, k

rozsahu kolektivu uživatelů, k jejich profesnímu charakteru, k typům možné motivace útoků, k rizikům průniku zvenčí či zevnitř atp.[29]

Dle anglické kampaně „Get Safe Online“ spočívá prevence počítačové kriminality na internetu v následujících krocích:

- instalace a aktualizace antivirového softwaru,
- instalace osobního firewallu,
- pravidelné zálohování dat,
- instalace oprav (záplat) operačního systému a aplikací,
- používání prostého textu místo HTML e-mailů,
- mazání spustitelných příloh,
- používání důmyslných hesel,
- šifrování elektronické komunikace,
- ignorace spamu a odkazů typu „Unscribe“ - ohlášení urážlivých, obtěžujících nebo podvodných e-mailů.

Prevence týkající se transakcí online:

- neprozrazovat hesla, PIN kódy, uživatelská jména apod.,
- nevyplňovat e-mailové formuláře,
- neklikat na odkazy v e-mailech,
- hledat na stavovém řádku prohlížeče symbol zámku,
- pravidelně kontrolovat bankovní účty a hlásit cokoliv podezřelého.

2.4.3 Technické a technologické prostředky počítačové bezpečnosti

Opatření v rámci počítačové bezpečnosti proti vnějším útokům, např. z externích počítačových sítí, jsou záležitostí převážně technického charakteru. Preventivní opatření tohoto typu je třeba centrálně koordinovat a postavit na předpisech obecně závazného bezpečnostního standardu. V České republice doposud tyto útoky ve větším rozsahu bezprostředně nehrozily, případně byly jen velmi málo pravděpodobné, protože zde dosud

[29] MATĚJKA, M. Počítačová kriminalita. Praha, 2002.

nejsou externí sítě příliš rozšířeny. Určitý prostor ale skýtá existence faxmodemových karet. Specifickým problémem je ochrana proti odečítání informací z vlnění vycházejícího z počítače. Útoky tohoto typu lze očekávat jen u dat s nejvyšším stupněm důležitosti. Lze jim čelit vhodným architektonickým řešením budov, v nichž počítače pracují, izolací zdí, krytů počítačů a dalšími technickými prostředky.

V případě technologické prevence se jedná v první řadě o zabezpečení. Na celou problematiku počítačové kriminality lze ve skutečnosti pouze s malou nadsázkou nahlížet jako na neustálou poziční válku mezi obránci a útočníky, mezi hackery a administrátory. Tvůrci ochran programů a systémů se snaží neustále vymýšlet nové a dokonalejší ochrany, kdežto hackeři a další se snaží tuto ochranu prolomit. Jedná se tedy svým způsobem o neustálý a nikdy nekončící boj. Tvůrci programů navíc často hackerům pomáhají tím, že vyrábějí chyby v programech, kterých je poté možno využít právě k prolomení ochrany systému. Působením technologické prevence nejenže nelze nad počítačovou kriminalitou zvítězit, ale nelze ani dosáhnout rovnováhy sil bez nutného spolupůsobení psychologické prevence. Nutnou podmínkou k tomu je především součinnost potenciálních obětí, tedy uživatelů a správců počítačů a sítí. Ti všichni se musí podílet na minimalizaci rizik plynoucích z počítačové kriminality. Uživatelé například tím, že nebudou spouštět podezřelé soubory získané z internetu či přílohy z došlých e-mailů, administrátoři zase musí pravidelně sledovat situaci, instalovat ochranné prvky, pravidelně aktualizovat antivirové programy apod.[30]

2.4.4 Nehmotné prostředky počítačové bezpečnosti

Zneužívání dat. Útoky směřující ke zneužití dat, neoprávněnému získání informací či způsobení změn, zničení dat apod., je bezesporu počítačovou kriminalitou velmi závažnou a u nás z hlediska dopadu poměrně opomíjenou. Přitom tyto útoky mohou mít velmi závažné důsledky. Nejedná se přitom jen o značné finanční ztráty, které mohou nastat dejme tomu peněžní instituci při nezákonných machinacích s daty, týkajících se finančních převodů. Může dojít i k jiným újmám, např. nehmotným, na osobnosti pachatele, na strategii vývoje podniku, na výrobě, na obchodních zájmech atp. Ochrana proti útokům tohoto typu tvoří stěžejní část počítačové bezpečnosti. Ke zvýšení počítačové bezpečnosti může přispět i dodatečné zjišťování neoprávněných průniků. To je však velmi obtížné.

[30] MATĚJKA, M. Počítačová kriminalita. Praha, 2002, s. 80.

V rámci organizačních opatření lze zvýšit počítačovou bezpečnost určitými omezeními v přístupu k výpočetní technice, zavedením vhodné evidence užívání systému, monitorováním práce uživatele, skartací výstupů tiskárny a jinými způsoby ochrany. Důležité je také stanovení způsobů tvorby, testování a předávání programových produktů pracovníků vlastní instituce dalším zaměstnancům. Obecně jde u organizačních bezpečnostních opatření o stanovení pravidel užívání výpočetní techniky a dat. Tato oblast by měla být dokonale zpracována ve vnitřním bezpečnostním standardu.

Instalace počítačových her. Určitým typem bezpečnostních organizačních opatření může být i oficiální instalace vybraných, regulérně pořízených počítačových her. Význam tohoto opatření spočívá ve snížení rizika vyplývajícího z donášení cizích, často pirátsky pořízených produktů s potenciální možností přenosů virů. Některé typy her mohou působit i jako náhražka pokusů o průnik „ze sportu“, protože jejich hraní je samo o sobě tak složité, že stačí uspokojit potřebu programátora překonávat překážky.

Jako součást opatření ke zvýšení bezpečnosti vůči útokům „zevnitř“ mohou být používány i některé méně tradiční metody, jako je např. vypsání soutěže o průnik do systému, který by odhalil slabiny jeho ochrany. Poněkud diskutabilní je metoda „líčení pastí“ se zdánlivou možností průniku k tajným datům s možností sledovat přitom chování uživatele.

Oblast personálních opatření by měla být zaměřena nejen na určitá kriteria výběru pracovníků, ale i na způsoby stabilizace kádru pracovníků a na opatření uplatňovaná při odchodu zaměstnance z instituce. Je třeba zlepšit i finanční hodnocení pracovníků zainteresovaných na bezpečnosti počítačových systémů, což mnohdy platové směrnice zatím neumožňují.[31]

2.5 Profil pachatele počítačové kriminality

Pachatele počítačové kriminality lze rozdělit z hlediska jejich vztahu k informacím, a to na:[32]

- *amatéry* – zde je možné zařadit hackery, crackery, neúspěšné kritiky a mstitele. Jde o osoby pronikající cílevědomě nebo náhodně do informačních systémů tak, že vyhledávají zranitelná místa. Jejich motivace a cíle bývají zpravidla různé.

[31] MATĚJKA, M. Počítačová kriminalita. Praha, 2002, s. 82.
[32] KŘÍŽ, L. X-vize budoucí bezpečnosti. 2006. Dostupný z http://www.computerworld.cz/cw.nsf/ID/B7AE352FC15C49A9C12570E9006B5837?OpenDocument&cast=1.

- *profesionály* – zde patří pracovníci speciálních tajných služeb, detektivové, žurnalisté, podnikatelé, specialisté informatici, softwaroví piráti či teroristé (zvláštní skupina organizovaného zločinu).

Někteří pachatelé počítačové kriminality provádějí trestnou činnost samostatně, ale ve většině případů se jedná o sdružování více osob do určitých skupin a jejich vzájemnou spolupráci. Jednotliví členové se většinou ani osobně neznají, neboť vzájemná komunikace probíhá elektronicky. Vztahy mezi jednotlivými skupinami, zabývající se touto trestnou činností, jsou poměrně komplikované.

Význam označení *hacker* prodělal v průběhu let pozoruhodný vývoj. Dříve byl hacker synonymem pro člověka, ke kterému se vzhlíží s úctou, dnes jej většina lidí považuje za pachatele trestné činnosti. Obecně lze říci, že hacker je člověk nadšený programováním, který se baví zkoumáním detailů a způsobů využití systémů a překonávání překážek je pro ně v tomto případě výzvou. Činnost hackera spočívá v pronikání do chráněných systémů s cílem prokázat své schopnosti a kvality bez zájmu získat informace, či nějakým způsobem narušit systém. Hackeři považují překonávání ochranných bariér za zábavu a dobrodružství. Typické pro opravdové hackery je jejich sociální chování, používaný jazyk, uznávání morálních hodnot a samozřejmě samotná činnost hackera, tedy hacking. Pojmem hacking je označována činnost, kterou hacker provádí a díky níž získává uznání a respekt. A to především získáním a zpřístupněním zdrojového kódu programů, odhalením slabin informačního systému a zpřístupněním příslušných informací, publikováním užitečných informací na internetu, pomoc při administrativě a provozu diskusních skupin, pomoc při testování nových programů atd. Pro zajímavost můžeme zmínit, že hacking, který není prováděn tak, aby způsobil někomu jinému škodu či jinou újmu nebo sobě či jinému neoprávněný prospěch, není kvalifikován jako trestný čin, a tudíž není postižitelný. Pro doplnění je ještě nutné uvést pojem hactivismus, který představuje politicky motivované napadání internetových stránek. V důsledku různých medializovaných kauz průniků do sítí se výraz „hacker“ vžil jako nálepka pro vandalství a poškozování informačních a komunikačních systémů.

Označení *cracker* se objevilo v souvislosti s pojmem crack, který představuje narušení zabezpečení ochrany a integrity programu nebo systému. Crackeři jsou osoby, které jsou schopné prolomit kód určitého softwaru a umožnit tak jeho nelegální kopírování, ale také osoby, které pronikají do počítačových systémů s úmyslem jejich poškození. Naproti tomu cracking je činnost, kdy dojde k prolomení ochrany určitého softwaru, tedy k narušení informačního systému zvenčí. Zpravidla cracker nepracuje sám, ale ve skupinách. Každý člen

má na starosti konkrétní činnost, bývají zpravidla hierarchicky rozděleni. Většinou bývají jednotlivé skupiny rozděleny tematicky. Specializují se např. na herní oblasti, na weby a různé počítačové aplikace. Mezi skupinami panuje obrovská rivalita, vzájemně mezi sebou soutěží, své úspěchy pečlivě dokumentují a zpravidla také zpřístupňují ostatním uživatelům na internetu. Crackeři se sami často považují za hackery, avšak jejich znalosti informačních systémů, internetových protokolů a programování nejsou na tak vysoké úrovni jako u hackerů. Crackeři používají k průniku do informačních systémů především zveřejněné slabiny, na které ještě administrátoři nezareagovali. Zásadní rozdíl, odlišující tyto patogenní osobnosti od hackerů, spočívá v pronikání do systémů s cílem data získat a následně zneužít ve vlastní prospěch. K těmto charakteristikám lze ještě přiřadit potěšení z destrukce systému.[33]

Pro získání celkového přehledu osob pohybujících se ve světě digitální kriminality existují další pojmy:

- *samuraj* – útočník, který pronikne do systému, avšak následně správci oznámí bezpečnostní nedostatky a poskytne mu konkrétní rady,
- *script-kiddies* – začínající útočníci s průměrnými znalostmi, kteří dokáží na internetu najít kód a mírně ho upravit, např. pro spuštění nové varianty viru (převážně využívají nástroje vytvořené jinými útočníky - skripty),
- *packet monkeys* – nezkušení uživatelé, kteří provádí útoky nevyžadující prolomení ochrany,
- *phreaker*/*phracker* – útočník, který proniká a zneužívá telefonních sítí,
- *phisher* – útočník, který vytváří identické webové stránky většinou různých finančních institucí a poté ukradne a zneužije citlivé údaje uživatelů, kteří je zadají v domnění, že jde o oficiální stránky instituce,
- *knacker* – útočníci, který odstraňují ochranný kód programů za účelem jeho volného používání,
- *looser*/*lamer* – uživatelé neznalí prostředí IT.

[33] SVETLÍK, M. Informační bezpečnost: část 1-4. Softwarové noviny. 2002, č. 2-5.

V literatuře zahraničních autorů se lze setkat také s pojmy:[34]

- *white hats* – tzv. „hodní“ hackeři, kteří nezpůsobují žádné škody a upozorňují administrátory systémů na objevené bezpečnostní chyby, někdy jsou také označování jako „ethical hackers“ – jde tedy o hackery v pravém slova smyslu,
- *black hats* – hackeři s kriminálními motivy, účelem je vlastní obohacení – jde tedy o tzv. crackery,
- *grey hats* – šedá zóna hackerů stojící na pomezí mezi předchozími typy, typické je pro ně zveřejňování bezpečnostních děr, tzv. exploitů v internetu za účelem růstu úrovně bezpečnosti systémů (výše uvedený samuraj),
- *elite* – hackeři proslavení nejlegendárnějšími kousky.

[34] TOLAR, O. Policie je krátká na weby popírající holocaust. 2006. Dostupný z http://zpravy.idnes.cz/krimi.asp?r=krimi&c=A060222_114752_krimi_ton.

3 Ekonomické a právní důsledky počítačové kriminality

Počítačová kriminalita je jedna z nebezpečných forem kriminálních deliktů a z hlediska nebezpečnosti pro společnost je srovnatelná s organizovaným zločinem. Počítače mnohdy pachatelům usnadňují či umožňují urychlit páchání trestné činnosti a výrazně snižují riziko jejich odhalení. Počítače jsou zneužívány ke klasické hospodářské trestné činnosti zejména tam, kde by manipulace s daty byla bez počítače složitá, zdlouhavá nebo v reálném čase nemožná. Patří zde např. realizace hazardních finančních her a podvodných investičních záměrů. Další velkou třídou možností využití počítače v kriminálním prostředí je oblast padělání a zhotovování falešných papírů, dokladů, platebních instrumentů aj. Vše samozřejmě v náležité kvalitě a vysoké věrohodnosti, což zejména moderní textové a grafické editory umožňují velmi snadno. Významnou charakteristikou pro počítačovou kriminalitu jsou v důsledku značné ztráty, ať již přímo v podobě finančních částek nebo v podobě zneužití získaných údajů.

3.1 Dopad počítačové kriminality na společnost

Počítačová a informační kriminalita se vymyká běžným vyšetřovacím postupům a proto je její objasnění zdlouhavější a dopad na společnost, ekonomiku a právní systém státu o to značnější. Digitální stopy jsou velmi proměnlivé, vysoce objemné a mohou být rozptýleny na velkém geografickém prostoru. Zajistit napadený hardware, tedy počítače a další výpočetní techniku, jako důkazní materiál, je většinou velmi problémové, protože by to znamenalo další ztráty pro poškozené oběti. Škody a ztráty, které jsou způsobeny počítačovou kriminalitou, zejména tedy kriminalitou, související s duševním vlastnictvím, se zjišťují, resp. vyčíslují velmi obtížně. K analýze a dešifrování digitálních stop je často nutný certifikovaný a specializovaný hardware či software, který bezpečnostní složky postrádají. Pravidlem zůstává obecně velmi nízká úroveň akceptace digitálních stop v právní praxi. Také zákony, které postihují kriminální chování v kybernetické oblasti, jsou stále pouze ve vývoji a existují spíše ve fragmentech.

Základní hodnota, která ovlivňuje stav kybernetické kriminality v zemi, je vzdělanost a vybavenost společnosti v oblasti informačních technologií. Společnost lze hypoteticky rozdělit na dvě skupiny. Ta první používá IT velmi intenzivně, nevěnuje však pozornost zabezpečení a kybernetické ochraně. Ta druhá nepoužívá IT vůbec. Je evidentní, že první

skupina se stane terčem pro kybernetické útoky, zatímco druhou skupinu to vůbec neovlivní. Ve skutečnosti se však celá naše společnost nachází někde uprostřed mezi těmito hypotetickými stavy. Informovanost o bezpečnosti a možných útocích je zhruba ve všech vyspělých státech na stejné úrovni. Důvodem je existence samotného kyberprostoru, ve kterém se informace šíří velmi rychle a jeho samotný charakter. Odlišným faktorem je v tomto případě legislativní připravenost společnosti a schopnost implementace legislativy policejními a justičními složkami. Zde však není možné dojít k celosvětově srovnatelnému stavu, protože v každém státě platí jiný právní systém, jiná morálka a je zde především odlišný historický a kulturní vývoj.

V důsledku počítačové kriminality přicházejí firmy každoročně na tržbách o miliardy dolarů. Podle celosvětové studie vypracované na objednávku organizace BSA přesáhly celkové ztráty softwarového průmyslu na celém světě v roce 2007 jako přímý důsledek softwarové kriminality 40 miliard dolarů. Společnost si neuvědomuje, že negativní důsledky kybernetické kriminality dalece přesahují samotného vydavatele softwaru. Ekonomické ztráty pociťují nejen výrobci softwaru nebo distribuční společnosti, ale především zákazníci, tedy samotní uživatelé.[35]

3.1.1 Klasifikace počítačové kriminality podle dopadu konkrétního skutku

Klasifikovat tuto problematiku není s aktuálně platnou legislativou vždy jednoduché. Počítačové delikty je možno strukturovat podle zamýšleného účinku nebo podle chráněného zájmu, který bývá napaden. V rámci tohoto dělení lze rozeznat:

- trestný čin proti osobě, kam patří útok proti pověsti, pomluva, vydírání, obtěžování, krádež identity, nenáležité nakládání s osobními údaji apod.,
- trestný čin proti vlastnictví, kde je možné rozeznat následující případy:
    - přímým dopadem činu je další obohacení se na úkor poškozeného,
    - následkem činu je naopak „úspora“ nákladů útočníka, jež by jinak byla ziskem postiženého (např. investice do koupě softwaru),
    - zisk útočníka a ztráta poškozeného spočívá v dalším nezákonném šíření neoprávněně získaných dat,

[35] JIROVSKÝ, V.; HNÍK, V.; KRULÍK, O. Kybernetické hrozby: výzva pro moderní společnost. 2008. Dostupný z http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/kyberneticke_hrozby.pdf.

- škoda napadeného subjektu je odvozena od vratného či nevratného zničení, poškození či pozměnění jeho dat,
- škoda je založena na zneužití informace, která byla neoprávněně získána z informačních a komunikačních sítí v reálném světě;

- trestný čin proti veřejnému zájmu, veřejnému pořádku nebo mravnosti, kam lze zahrnout pobuřování, šíření poplašných zpráv, kybernetický terorismus, politicky motivovanou špionáž, šíření nelegální pornografie, šíření nenávisti, schvalování zločinu a nabádání k němu nebo propagaci toxikomanie apod.

Z výše uvedeného vyplývá, že jednotlivé části této klasifikace se i v těch nejmenších detailech navzájem prolínají. Je to však pouze jedno z možných rozdělení a samozřejmě není vyčerpávající. Je zřejmé, že jakákoliv taková strukturalizace není vhodná pro jednoznačné určení, o jaký konkrétní trestný čin se jedná. Aby došlo k minimalizaci finančních i časových nákladů při potírání počítačové kriminality, mohly by se, dle mého názoru, v praxi všechna jednání řadit do jedné kategorie. Nejsnadnější by bylo přesně specifikovat jednotlivé skutkové podstaty kybernetické kriminality. Tyto skutkové podstaty by se případně mohly objevit v jednotném oddílu, který by nesl název např. počítačové trestné činy. Ze zhodnocení současné úpravy trestního zákoníku vyplývá, že dosud žádná část není věnována právě a jen této trestné činnosti. Všechna ujednání, která vypovídají o skutkových podstatách kybernetických trestných činů, jsou v trestním zákoníku velmi nerovnoměrně uspořádána.

3.2 Počítačová kriminalita v České republice a v zahraničí

Stejně jako ostatní země světa se Česká republika setkává s problémy počítačové kriminality. Patříme ke státu, kde je stav kybernetických zločinů průměrný. Možnosti preventivních a represivních složek jsou rozdílné a odvíjejí se od vyspělosti informačních technologií, zkušeností a možností vzájemné spolupráce. Ve vyspělých zemích vznikají speciálně školené týmy, které mají za úkol právě boj s kyberzločinem. Jejich působnost dosahuje většinou úrovně jednotlivých území, případně vyšších úrovní jednotlivých územních celků. V České republice se o potírání počítačové kriminality stará odbor informační kriminality úřadu služby kriminální policie a vyšetřování a dále jednotlivá oddělení

informační kriminality na krajských ředitelstvích Policie České republiky.[36] Pro oblast informačních technologií je u nás zřízen vrcholový orgán státní správy – Ministerstvo informatiky. Obecně lze říci, že v legislativě naší republiky neexistuje žádný konkrétní zákon vztahující se právě k počítačové kriminalitě. Veškeré problémy a stanoviska jsou roztroušeny v mnoha různých právních předpisech a to ne vždy úplně ideálně. Neexistuje tedy jednotný a ucelený pohled na tuto problematiku. V některých případech se vůbec nepočítá s trestnými činy páchanými pomocí počítače, jelikož v této oblasti vznikají stále nové neprozkoumané možnosti a to především díky prudkému a neustálému rozvoji informačních technologií. Díky tomu nejsou kyberzločiny vždy dostatečně definovány a nejsou určeny jejich přesné skutkové podstaty.[37]

Mezi konkrétní trestné činy, které jsou nejvíce zastoupeny v České republice, patří[38] (řazeno podle četnosti a závažnosti):

- zakázaná pornografie,
- extremistické projevy,
- zneužití platebních a obchodních systémů v internetu,
- porušování autorského práva,
- pomluvy a diskreditace osob,
- zneužívání dat, včetně útoků na data,
- podvodné e-maily, spamy.

Z aktuálně platné legislativy vyplývá, že žádná z evropských zemí není na současný stav komunikačních a informačních technologií dostatečně připravena. Jednotlivé případy jsou vyšetřovány z různých hledisek a slepovány z mnoha zdrojů a celkový koncept této oblasti je teprve ve stádiu zrodu. O mnoho lépe na tom není ani zahraniční legislativa. Je však o krok napřed z důvodu odlišné právní metodiky, která spočívá v právních precedentech a dodatcích Ústavy. Proto má již pro jednotlivé trestné činy této oblasti své vzory.

[36] KUCHAŘÍK, K. Činnost policie ČR ve vztahu k informační kriminalitě. Dostupné z i.iinfo.cz/… /Karel_Kucharik_-_Cinnost_Policie_CR_ve_vztahu_k_informacni_kriminalite-123572804005458.ppt.
[37] PAUKERTOVÁ, V. Elektronická informační kriminalita. 2006. Dostupné z http://www.ikaros.cz/node/3554.
[38] AMBROŽ, J. Jak silná je naše „softwarová policie“? Dostupné z http://www.lupa.cz/clanky/jak-silna-je-nase-softwarova-policie/.

3.2.1 Právní úprava počítačové kriminality v České republice

Nejdůležitějšími a základními zákony, které jsou v problematice počítačové kriminality uplatňovány nejčastěji, jsou:

Obchodní zákoník

Zákon č. 513/1991 Sb., v podobě, která začleňuje poslední novely. Upravuje postavení podnikatelů, obchodní závazkové vztahy, jakož i některé jiné vztahy, které s podnikáním souvisejí. Jeho uplatnění nastává zejména v případech, kdy nelegální aktivity souvisí se smluvním nebo podobným vztahem upraveným v tomto zákoně.[39]

Občanský zákoník

Zákon č. 40/1964 Sb. Tento základní předpis je důležitý zejména proto, že jednoznačně definuje jednak vlastnické právo a jednak entity, proti kterým je kriminální činnost namířena, právnické a fyzické osoby.[40]

Autorský zákon

Zákon č. 121/2000 Sb., Zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů. Tento zákon má za následek mnoho soudních procesů, kde se žalující domáhá autorského práva k programům, nebo podobným produktům. Autorský zákon chrání programy, data a nahrávky uveřejněné na internetu tím způsobem, že kdo je neoprávněně získá, zcizí, případně zneužije a následně opětovně uveřejní, ten se dopouští trestné činnosti. Záleží ale také na tom, o jaká data se jedná. Může jít např. o trestný čin ohrožení utajované informace (§ 317 TrZ), trestný čin související s ochranou osobních údajů (§ 180 TrZ), trestný čin porušování průmyslových práv (§ 269 TrZ), případně o porušení autorského práva (§ 270 TrZ). V České republice se jedná o oblast, která je v kyberprostoru nejvíce chráněna. V této oblasti již bylo také vydáno řádově desítky odsuzujících rozsudků.[41]

---

[39] Zákon č. 513/1991 Sb., obchodní zákoník.
[40] Zákon č. 40/1964 Sb., občanský zákoník.
[41] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů

Zákon o ochraně osobních údajů

Souvisí velmi úzce s ochranou telekomunikačního tajemství, ale má i určitou působnost v oblasti databází obsahující konkrétní údaje, které by mohly vést k jednoznačné identifikaci osoby. Zákon č. 101/2000 Sb., o ochraně osobních údajů, navazuje na směrnici 95/46/EC Evropského parlamentu a Rady z 24. října 1995 o ochraně jednotlivců v souvislosti se zpracováním osobních údajů a s volným pohybem těchto údajů. Ta zase vychází z Úmluvy č. 108 o ochraně osob se zřetelem na automatické zpracování osobních dat, kterou Česká republika podepsala dne 8. září 2000.[42]

Trestní zákoník

Jako nejdůležitější prostředek pro vyšetřování počítačové kriminality se jeví zákon č. 140/2009 Sb., trestní zákoník. Tento slouží jako represivní nástroj v okamžiku, kdy dojde k porušení některého zákonného předpisu, který spadá do sféry trestní odpovědnosti. V těchto případech se však bohužel stává, že výklad zákona je takový, že některé typické kriminální delikty v počítačovém prostředí se jen velmi obtížně začleňují do stávající osnovy zákona. Také sbírání důkazů je v takových případech poměrně složitá věc, neboť procesní dokazování je stavěno na klasických důkazních metodách.[43]

Zákon o regulaci reklamy

Zákon č. 40/1995 Sb., reguluje ve své poslední úpravě i některé elektronické problémy, např. spam.[44]

Zákon o elektronických komunikacích

Zákon č. 127/2005 Sb. nahradil původní telekomunikační zákon č. 151/2000 Sb. Pokrývá širokou škálu působení telekomunikačních a podobných společností na trhu, přičemž z kybernetického hlediska upravuje některé důležité aktivity související s případným nezákonným chováním subjektu v prostředí počítačové sítě. Součástí tohoto zákona je nejen podmínka dodržování telekomunikačního tajemství, ale i např. ustanovení zakazující používat automatických systémů bez lidské účasti pro účely přímého marketingu bez předchozího souhlasu dotčeného účastníka.[45]

[42] Zákon č. 101/2000 Sb., o ochraně osobních údajů.
[43] Zákon č. 140/2009 Sb., trestní zákoník.
[44] Zákon č. 40/1995 Sb., o regulaci reklamy.
[45] Zákon č. 127/2005 Sb. o elektronických komunikacích.

3.2.2 Současné kybernetické ohrožení České republiky

I když je Česká republika malou zemí, rozhodně nepatří mezi ty, kterým by se počítačová kriminalita vyhýbala. Internetová doména „.cz“ byla v minulosti několikrát vystavena útokům, resp. výhružkám na takový útok. Většina aktérů kybernetické kriminality má ke svým činům politické důvody. S rozvojem informačních technologií se rozmáhá také tento druh kriminality. Zůstává však většinou stranou veřejného zájmu. Až medializované případy přivedly veřejnost k nutnosti investic do kybernetické bezpečnosti.

- Informační technologie jsou stále ve větší míře využívány pachateli celého spektra trestné činnosti. Počet kybernetických incidentů všeho druhu bude v České republice stále narůstat (co do počtu případů, i co se týče jejich závažnosti a způsobených škod).
- Klesá počet incidentů motivovaných snahou o medializaci. Předpokládá se, že roste počet skrytých incidentů, usilujících o zisk.
- Přibývá pachatelů (expertů), zneužívajících svých znalostí za úplatu.
- Je zaznamenáván stále rostoucí výskyt nežádoucích materiálů, které jsou distribuovány prostřednictvím Internetu (počítačové programy, filmy, hudba, ale i materiály obsahující zakázané formy pornografie a extremistickou propagandu).
- Přetrvávají případy zneužívání telefonních linek se zvýšeným tarifem pro neautorizované přesměrování připojení koncových uživatelů Internetu.
- Je možné vysledovat nárůst případů zneužití elektronických nákupů.
- Byly zaznamenány případy zneužití internetového bankovnictví („phishing“, snaha o podvodné vylákání citlivých dat, ”skimming” platebních karet).
- Všechny uvedené činnosti vykazují vysoce latentní charakter.
- Není časté, aby v České republice docházelo k trestnímu stíhání pro incidenty, podřaditelné pod kybernetickou kriminalitu. Neděje se to proto, že by se takové incidenty nestaly, ale spíše proto, že jejich odhalení (a ještě více dokázání) je značně obtížné.[46]

Dle dokumentů Ministerstva vnitra České republiky patří v současné době k nejčastějším projevům počítačové kriminality porušování autorských práv, šíření extremistické a teroristické propagandy, šíření zakázané pornografie, podvodných jednání, výhrůžek, vydírání, šíření poplašných zpráv, pomluv a útoků na informační systémy a data. V rámci

[46] JIROVSKÝ, V.; HNÍK, V.; KRULÍK, O. Kybernetické hrozby: výzva pro moderní společnost. 2008. Dostupný z http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/kyberneticke_hrozby.pdf.

porušování autorských práv dochází k přesunu trestné činnosti z původně dominantního prostředí výměnných sítí do segmentu datových úložišť. Pro výměnu odkazů a také hesel ke komprimovaným materiálům s obsahem autorsky chráněných děl, šířených v rozporu s autorským právem, jsou využívána fóra, která jsou řazena tematicky. Čím dál obezřetněji ve vztahu k protiprávnímu jednání je využíván Internet extremisty. Oproti minulosti jsou na vzestupu projevy levicového extremismu. Extremisté k důraznějším a extrémněji laděným projevům a ke komunikaci již využívají uzavřených komunit, a to s dominantním zapojením sociálních sítí. Na neustálém vzestupu jsou také útoky formou tzv. phishingu.[47] Navíc se tak děje za souběžného zneužití předem vytvořeného prostředí ve formě tzv. botnetů,[48] tj. útokem vytvořených cílových stanic, určených přes různé sítě k páchání dalších kriminálních aktivit ve formě např. vedení masivních útoků, šíření spamů a prolomení ochrany systémů. Na území České republiky nebyl zjištěn výskyt organizátorů takovéto jednání, ale velmi častý je výskyt e-mules (tzv. „bílých koňů"), jejichž úkolem je převzetí neoprávněně odčerpaných prostředků z účtu poškozeného na svůj účet a ty pomocí jiných platebních toků poslat dále.

V roce 2010 byly neustále zaznamenávány snahy o umístění phishingových stránek. Ze stávajících poznatků je patrná snaha o realizaci vytváření elektronických obchodů, které budou vytvářeny primárně za účelem krytí zdrojů a původu financí pocházejících z trestné činnosti, zejména tedy z phisingových útoků a zneužitých čísel platebních karet.

Podle ÚOKFK PČR výrazně narostl v roce 2010 počet případů phishingu, v nichž pachatelé využívají území ČR, zejména Prahy a Středočeského kraje, k převodu[49] peněžních prostředků ze svých účtů určeným osobám do zahraničí, kdy tyto peníze pocházejí z organizované počítačové kriminality v zahraničí. V souvislosti s projevy pachatelů různých podvodných jednání je novým fenoménem skrývání své činnosti za cíleně vznikající společnosti. Vnitřní chod a struktura společnosti je stavěn tak, aby nebyla možná konkrétní identifikace jednotlivce a v rámci trestního řízení nebylo možno postupovat dále.

V souvislosti s *elektronickým obchodováním* se v minulém období projevil ve větší míře trend elektronických virtuálních obchodů, kde je realizováno v krátkém období velké množství transakcí. Po příjmu objednávek proběhne platba, ale již se dále nerealizuje dodání objednaného zboží a poté následně dochází k zániku aktivit obchodu bez dalších reakcí.

[47] Zaznamenávání přístupových kódů, sloužících zejména k podvodnému přístupu na bankovní účty, z nichž jsou pak neoprávněně odčerpávány finanční prostředky.
[48] Podle BIS Působení malware, který botnety vytváří, spočívá zpravidla ve sběru přihlašovacích a jiných citlivých údajů i bez použití phishingu. Daleko významnější využití botnetů zřejmě spočívá v distribuci spamu a malware, přímým elektronickým útokům a přímému sběru přihlašovacích údajů.
[49] Nejčastěji se jedná o trestné činy legalizace výnosů z trestné činnosti nebo legalizace výnosů z tr. činnosti z nedbalosti.

V rámci *šíření zakázaných forem pornografie* je zřejmé, že dochází k tomu, že se vytváří uzavřené komunity. Co se týká prověřování svých členů, neustále se zdokonalují. Následně dojde k takové situaci, že jsou dané materiály šířeny s velkou latencí a to především přes e-mail a úložný prostor. Detekce takových aktivit vyžaduje větší nasazení vlastní agenturní činnosti, aby bylo možno se do daných komunit infiltrovat. V souvislosti s dětmi se také začíná objevovat snaha pachatelů získávat materiály skrz síť Internet. Jedná se hlavně o fotografie a ostatní materiál pornografického charakteru.

Postupem času dochází k profesionalizaci pachatelů počítačové kriminality. Začínají využívat taktiku tzv. sociálního inženýringu, což je činnost, během které si pachatelé vyhledávají své oběti zvláště prostřednictvím chatů a sociálních sítí. Objevují se ale také případy, kdy samotné děti vyhledávají, cíleně zobrazují a nabízejí materiály, které mají charakter dětské pornografie, za peníze a jiné odměny. Typickým příkladem takového benefitu je dobití kreditu do mobilního telefonu.

Bezpečností rizika vyplývající ze znemožnění zjištění identit pachatelů jsou především šíření anonymního připojení do sítě Internet prostřednictvím volně přístupných Wi-Fi bodů a přetrvávání anonymního připojení z předplacených karet mobilních operátorů. Hrozí nebezpečí anonymizovaných komunikací zneužitelných zejména k šíření poplašných a výhružných zpráv a k realizaci organizovaného zločinu.

Oproti roku 2009 se v roce 2010 zvýšilo na dvojnásobek množství škodlivého software (malware) a spamů. Významný podíl na tomto navýšení má masivní rozšíření komunikace prostřednictvím sociálních sítí, které se staly nejrozšířenějším prostředkem k uplatňování většiny typů kybernetických hrozeb. Technická úroveň škodlivého software se neustále zvyšuje a tím také složitost jeho detekce a obrany. Autorství takového software se poté přesouvá od vzdělaných jedinců k organizovaným skupinám. Tyto skupiny jsou podporovány organizovaným zločinem. Zvyšuje se podíl specializovaných útoků na konkrétní cíle. Motivace bývají různé, většinou finanční, politické a ideologické.

V oblasti kybernetické kriminality České republiky zůstává problémem velmi nízká úroveň povědomí o informační bezpečnosti, i když se pomalu zvyšuje. Stále přetrvává názor, že bezpečnost snižuje efektivitu provozu informačních technologií. V roce 2010 nastal pozitivní vývoj v otázce ustanovení subjektu odpovědného za otázky kybernetické a informační bezpečnosti ČR.

Koordinátorem a gestorem za tuto oblast a zároveň „národní autoritou“ se stalo 15. dubna 2010 Ministerstvo vnitra přijetím usnesení vlády České republiky ze dne 15. března 2010 č. 205. Byl ustaven Odbor kybernetické bezpečnosti. S ohledem na složitost a šíři problematiky

kybernetické a informační bezpečnosti, je personálně, finančně, technicky a systémově tato oblast nadále trvale podhodnocena.[50]

3.3 Kriminalita na internetu a kyberterorismus

S rostoucím počtem uživatelů internetu roste i počet spáchaných trestných činů, které s ním nějak souvisí. České zákony na ně reagují se zpožděním, a tak někdy dochází ke sporným situacím.[51] Studie, kterou zveřejnil výrobce bezpečnostního softwaru Norton, odhaluje šokující rozmach počítačové kriminality.[52] Dvě třetiny (65 %) uživatelů Internetu na celém světě a téměř tři čtvrtiny (73 %) uživatelů webu v USA se již někdy stalo obětí počítačové kriminality, včetně počítačových virů, zneužití kreditní karty online a krádeže identity. Podle těchto údajů jsou Američané jedním z nejvíce postižených národů a zaujímají druhé místo za Čínou. Tato studie také objasňuje důsledky počítačové kriminality na osobní život obětí. Zkoumá emoční dopad počítačové kriminality, ukazuje, že nejvýraznější reakcí oběti je pocit hněvu (58 %), rozzlobenosti (51 %) a podvedenosti (40 %) a že oběti dávají útok v mnoha případech za vinu sobě. Pouze 3 % respondentů si nemyslí, že se to přihodí také jim, a téměř 80 % neočekává, že budou počítačoví zloději postaveni před soud. Výsledkem je paradoxní nechuť podniknout něco na svoji obranu a pocit bezmoci.

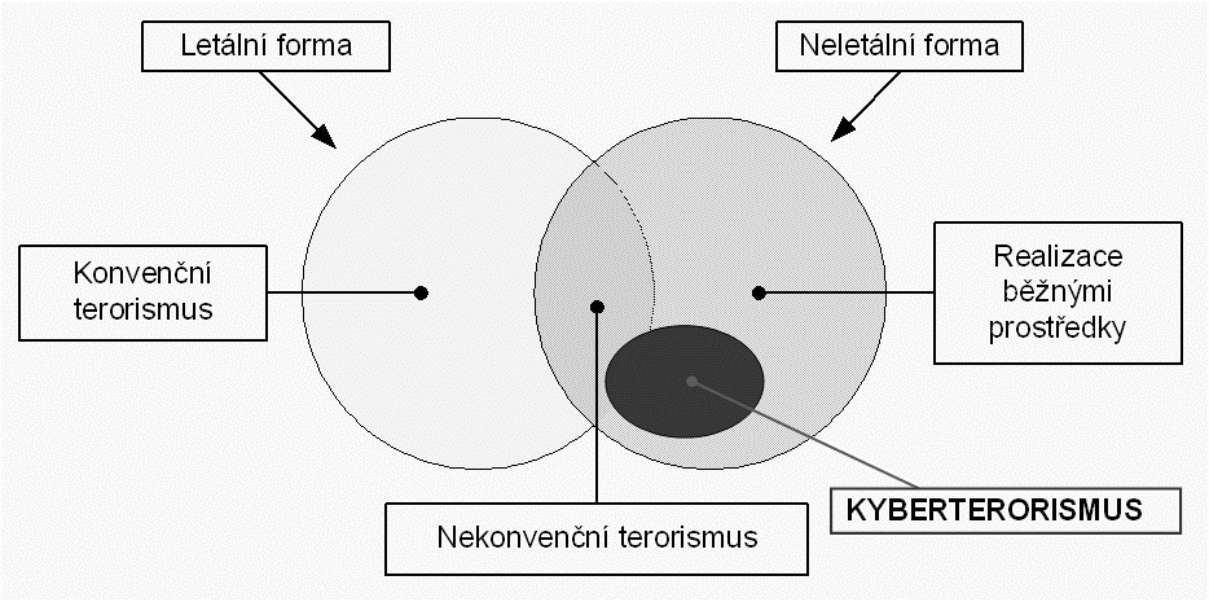
Terorismus ve světě představuje hrozbu, která se v posledních letech rozrůstá do různých podob. Dnes není pojem terorismus pouze politicky motivovaný atentát, ale odráží se v mnoha faktorech a mnoha úrovních lidského konání. Jelikož fenoménem moderní společnosti je schopnost využívání informací, objevuje se také velmi specifický a nebezpečný druh skryté hrozby – kyberterorismus. Vznikem internetu a novým systémem práce s informacemi se začíná hovořit o „informační společnosti“. V obecné rovině se tímto pojmem *„rozumí společnost, kde kvalita života i perspektiva sociálních změn a ekonomického rozvoje závisí na informacích a schopnosti jejich využívání, tj. informace se stává klíčovým faktorem takovéto společnosti.“*[53] Informační společnost se pohybuje v tzv. kyberprostoru, který byl definován Williamem Gibsonem z roku 1984. Je vymezen takto: „*Konsensuální*

[50] Ministerstvo vnitra České republiky. Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2010. Praha 2011, s. 58. Dostupné z www.mvcr.cz/soubor/zprava-komplet-2009-pdf.aspx.
[51] KUCHAŘÍK, K. Kriminalita na internetu. Dostupné z http://info.muni.cz/txt/1009/19.html.
[52] MOUNTAIN VIEW**:** Nenápadná epidemie: počítačová kriminalita postihuje více než dvě třetiny uživatelů Internetu. Dostupné z http://www.symantec.com/cs/cz/about/news/release/article.jsp?prid=20100908_02.
[53] DYTRT, Z.; MIKULECKÝ, P.; NEJEZCHLEBA, M.; PRILLWITZ, G.; ROUDNÝ, R. Etika podnikání a veřejné správy: Informační společnost – etická výzva pro 21. století. Praha. 1999.

halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky. Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v ne-prostoru mysli, shluky a souhvězdí dat."[54] Současnou společnost je možné považovat v ideálním stavu za informační, protože téměř každý člověk zná internet a počítač, tudíž má přístup k informacím a dokáže je využívat. Dnes je pojmem kyberprostor označován svět virtuální reality, v němž se odehrávají různé věci, např. komunikace prostřednictvím e-mailu, telefonické hovory, apod. Obecně označuje běžný uživatel tento kyberprostor pojmem internet. Ten však označuje pouze určitou konkrétní část virtuální reality kyberprostoru.

Kyberprostor musí díky své rozsáhlosti čelit určitým hrozbám. Jednou z nich je již zmíněný kyberterorismus. Jedná se o neletální formu teroristické činnosti realizovanou skrze informační a komunikační síť. Neletální forma je však jen vnějším obalem, protože následkem kybernetického útoku se může stát také fyzická likvidace konkrétního systému nebo objektu, což může vést i ke ztrátám na lidských životech. Většinou se však nejedná o primární cíl takového útoku.

Obr. č. 1 Grafické začlenění pojmu kyberterorismus do množiny terorismu



Zdroj: JÍROVSKÝ, V. Kyberterorismus. ICTfórum/PERSONALIS 2006. [předneseno 27.9.2006]. Praha. Vlastní zpracování, 2011.

[54] Kyberprostor. Wikipedia – the Free Encyclopedia. Dostupné z http://en.wikipedia.org/wiki/Cyberspace.

Oficiální definice kyberterorismu od D.E.Denninga zní následovně: *„Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.“*[55]

Tato definice je však poněkud zavádějící, neboť chápe pojem kyberterorismus jako akty směřované proti nějaké infrastruktuře, které si kladou za cíl získat jistou informační nadvládu. Mnohem častěji se však objevují útoky, které se snaží narušit fungování určité služby nebo jejich součástí, aniž by šlo o to, poškodit konkrétní společnost či vládu.

Kyberterorismus se dá podle svého působení rozdělit na dva směry:[56]

- první směr je čistě propagandistický a směřuje k negativní či odmítavé reakci na aktuální stav mezinárodní či národní politické situace (propagace jednotlivých teroristických skupin, propagace ideologií apod.)
- druhý směr realizuje přímá napadení konkrétních informačních sítí a likvidace síťových služeb a je tudíž výrazně nebezpečnější, neboť ve své snaze útočník většinou paradoxně zničením sítě nebo její části zlikviduje i svůj operační prostor.

Obecnou kategorizaci využití informační sítě pro teroristické potřeby lze rozdělit do tří úrovní:

- *vnitřní řízení* – teroristická skupina využívá informačních technologií k řízení svých lidských zdrojů, rozptýlených po celém světě. Zde typicky patří např. využití steganografie (skrytí textu do obrázků) pro předávání úkolů a reportů mezi jednotlivými členy skupiny.
- *lokální kyberútok* – samostatný přímý útok na konkrétní technologii či službu. Nebezpečnost tohoto druhu útoku je závislá na zkušenostech, cílech a možnostech dané skupiny. Pro vedení útoku jsou potřeba zkušení uživatelé síťových služeb a IT specialisté, kteří mají potřebné znalosti a zkušenosti v oblasti bezpečnosti počítačových sítí.
- *souběžný útok* – nejnebezpečnější varianta útoku, kdy dochází k několika paralelním útokům na konkrétní oblasti či cíle na různých úrovních. Kybernetický útok v této fázi

[55] DENNING, D. E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Dostupné z http://www.nautilus.org/infopolicy/ workshop/papers/denning.html.
[56] JANOUŠEK, M. Kyberterorismus: terorismus informační společnosti. Dostupné z http://www.army.cz/mo/obrana_a_strategie/2-2006cz/janousek.pdf.

je pouze jakousi přípravou pro napadení útočníka nebo přímou podporou pro jeho dezorientaci a likvidaci, která může být v přímé součinnosti s přímou akcí speciálních jednotek nebo např. leteckým bombardováním či dělostřeleckou přípravou. Může také docházet ke koordinaci několika různých druhů útoků.

3.3.1 Kyberšikana

Informační technologie se staly běžnou součástí každodenního života a to také u dětí. Již ze samotného názvu je zřejmé, že se jedná o specifický druh šikany. Na rozdíl od klasické šikany, nabízí kyberšikana agresorům nejenom jiné nástroje ubližování, ale specifika virtuální reality obměňují charakter celého procesu šikanování, včetně rolí agresora a oběti.[57] Kyberšikana je tedy definována jako úmyslné, opakované a nepřátelské chování jednotlivce nebo skupiny, podněcující k násilí vůči ostatním skrze informační a komunikační technologie.[58] Kyberšikana může mít různou podobu. Může jít o zasílání výhružných a krutých e-mailů a SMS zpráv, výhružné telefonáty nebo obtěžování přes online chat. Vytváření webových stránek, které různými způsoby (verbálně, graficky, nebo zvukově) oběť šikany urážejí a zesměšňují, je také jedním z projevů šikany na Internetu. Objevují se také případy, kdy agresoři získají hesla a identifikační údaje oběti a pod jejím jménem zasílají ostatním uživatelům vulgární a obtěžující zprávy, nebo fotografie a videa. Fotografování a nahrávání oběti, kdy jsou pořízené záběry posílány spolužákům, je také forma kybernetické šikany.

Většina obětí kyberšikany se nikdy nedozví, kdo je šikanoval, neboť přezdívka, anonymní telefonní číslo, či e-mailová adresa dávají agresorovi dostatečnou možnost zůstat skrytý. Díky tomu může útočník svou agresi stupňovat a dovolit si to, co by si za situace „tváří v tvář“ nedovolil. Agresorem nebývají většinou fyzicky zdatní lidé, tak jak tomu bývá u běžné šikany. Zde jde především o člověka, který má dostatečné znalosti z oblasti informačních technologií. Obětí útoku je většinou outsider, ale nebývá to pravidlem. Útočník si své oběti může vybírat náhodně, ale větší riziko hrozí dětem, které jsou na svém mobilním telefonu, případně počítači závislé. Klasická šikana se většinou odehrává v kolektivu dětí, tedy ve škole nebo při cestě domů. Jedná se tedy o fyzická setkání, která se dají předvídat a je možné se jim částečně vyhnout. Před kyberšikanou však není úniku, neboť agresor může svou oběť

[57] Šikana a kyberšikana. Dostupné z http://proti-sikane.saferinternet.cz/sikana-a-kybersikana.
[58] Virtuální ponižování aneb kyberšikana. 2010. Dostupné z http://www.inflow.cz/virtualni-ponizovani-aneb-kybersikana.

kontaktovat prakticky kdykoliv. Jelikož kyberšikana postrádá klasické znaky šikanování, kterých by si mohli dospělí všimnout, znesnadňuje tím kontrolu hlavně ze strany rodičů. Divákem kybernetické šikany se může díky webovým stránkám stát téměř kdokoliv na světě.[59]

Kyberšikana je natolik závažným problémem, že se boj proti ní stal hlavním tématem celoevropského Programu pro bezpečnější internet na roky 2009 až 2013. Jeho součástí jsou také české projekty Saferinternet.cz a Protišikaně.cz. V mnoha zemích jsou přijímána různá opatření v boji s kyberšikanou. Polsko např. filtruje na školních sítích přístup k Internetu a zakazuje ve školách používání mobilních telefonů, Jižní Korea ustanovila speciální policejní vyšetřovací týmy určené pro boj s kyberšikanou a v USA je kyberšikana od roku 2006 federálním zločinem.

Státem ratifikovaná Úmluva o právech dítěte zaručuje všem dětem v pedagogických zařízeních bezpečný pobyt bez poškozování zdraví a ohrožení života. Šikanování je tudíž v řadě případů trestnou činností. Šikana může naplňovat skutkovou podstatu trestných činů, např. omezování osobní svobody, krádeže, ublížení na zdraví, poškozování cizí věci, vydírání, loupeže, rasově motivované skutky, znásilnění, pohlavní zneužívání apod. Osoba mladší 15 let není trestně odpovědná, ale soud pro mládež ji může uložit podle zákona č. 218/2003 Sb., (o soudnictví ve věcech mládeže) některá z následujících opatření: dohled probačního úředníka zařazení do terapeutického, psychologického nebo jiného vhodného výchovného programu ve střediscích výchovné péče a ochranná výchova. Trestní odpovědnost mladistvých (15-18 let) je posuzována soudy pro mládež podle zákona č. 218/2003 Sb. s ohledem na rozumovou a mravní vyspělost osoby, proti níž se vede trestní řízení. Po dovršení 18 let věku jsou osoby plně trestně odpovědné a projednávají se běžným způsobem v trestním řízení.[60]

V České republice vznikl výzkumný tým a realizoval projekt E-Bezpečí. Spolu s Centrem prevence rizikové virtuální komunikace provedl v roce 2009 výzkumné šetření, zaměřené na výskyt nebezpečných komunikačních jevů spojených s využíváním informačních a komunikačních technologií. Do výzkumného šetření se zapojilo téměř 2000 respondentů z celé České republiky. Závěry českého výzkumu bohužel potvrdily to, co dlouhodobě naznačují také výsledky zahraničních výzkumů prováděných např. v USA, Velké Británii a dalších zemích - *téměř polovina českých dětí je vystavena některé z forem kyberšikany (46,8*

[59] KŘESŤANOVÁ, L. Kyberšikana, aneb Nikdy nevíš kdo je na druhé straně. 2009. Dostupné z http://ruce.cz/clanky/595-kybersikana-aneb-nikdy-nevis-kdo-je-na-druhe-strane.
[60] POLICIE ČR. Šikana. 2010. Dostupné z http://www.policie.cz/clanek/preventivni-informace-sikana.aspx.

%). V rámci výzkumu byly sledovány nejčastější projevy kyberšikany, mezi které patří např. *dehonestující útoky* (nadávání, urážení nebo ponižování realizované pomocí SMS zpráv, e-mailů, v online chatu, diskuzi a publikací zesměšňujících fotografií, audio nebo audiovizuálních nahrávek), *vyhrožování a vydírání*, *útoky na elektronické účty* (e-mailové, diskusní, účty ke vzdělávacímu prostředí atd.) *a jejich manipulaci, případně zneužití např. ke kyberšikaně*. Z těchto projevů jsou děti nejčastěji vystaveny nadávkám, urážkám nebo ponižování v rámci SMS zpráv, e-mailů, v chatu nebo diskuzi (15,8 %), dále musí řešit např. napadení svého elektronického účtu (13,5 %) nebo výhrůžky a zastrašování (8,9 %).

4 Ochrana dat

4.1 Ochrana dat v informačních systémech

S počítačovou kriminalitou souvisí bezprostředně také ochrana informací a dat v informačních systémech.[61] Nebezpečí datům hrozí nejen při jejich ztrátě, ale i při tom, když si je přečte někdo nepovolaný. Nejde jen o to nenechávat diskety, CD nebo USB paměti s důležitými daty ležet volně na stole, ale třeba i o to, aby neoprávněná osoba nedostala přístup k osobním datům na počítači. Něco takového se může snadno stát. Bezpečnost dat rozhodně není jen záležitost lidí pracujícími s počítači, ale zahrnuje všechny zaměstnance firem. Bezpečnost informačního systému je nejen ve firmách velmi důležitá. Stojí na dvou pilířích. Hlavním nosným dokumentem je bezpečnostní politika, která popisuje všechny bezpečnostní aspekty, se kterými je možné se v daném prostředí setkat - zabezpečení stanic, serverů, sítě jako celku, autentizaci uživatelů, jejich přístup k síťovým zdrojům atd. Bezpečnostní politika je vytvořena na základě komplexního bezpečnostního auditu, který provádí certifikovaný autor informačních systémů. Pro úspěšnou implementaci bezpečnostní politiky je nutné, aby byla podporována vedením firmy, které má na zabezpečení informací v informačním systému zájem. V praxi se bezpečnostní politika projevuje vydáním závazných směrnic, které přesně z bezpečnostního pohledu specifikují, co kdo může a co nikoliv. Samozřejmě je nutné vynucovat dodržování těchto směrnic. Na úrovni operačního síťového systému je zabezpečení dat realizováno systémem přístupových práv. Přístupová práva zajišťují nebo odepírají přístup autentizovaného uživatele k souborům a adresářům na diskových médiích stanic a serverů. Každý síťový operační systém takovým systémem disponuje. Pro další úroveň zabezpečení, zejména citlivých dat, je možné použít šifrování. V současné době je standardizováno velké množství šifrovacích algoritmů, které spolehlivě zabezpečí data před neoprávněným přístupem, tedy před přístupem bez vlastnictví šifrovacího klíče. Bezpečnost jako taková se týká i manipulace se zálohovacími médii, zahrnuje pravidla pro práci s přenosnými zařízeními, týká se přenosů dat a řady dalších aspektů používání výpočetní techniky.[62]

Všechny informační systémy jsou založeny na využívání jisté báze dat. Data jsou uložena v tabulkách databází, v souborech na disku, jsou přenášena elektronickou poštou, převáděna

[61] POŽÁR, J. Některé trendy informační války, počítačové kriminality a kyberterorismu. Dostupný z http://www.svses.cz/skola/akce/konf/bezp05/texty/pozar.pdf.
[62] DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. 2004.

na papír a rozesílána běžnou poštou a podobně. Ne všechna data by měla být přístupná všem lidem, některá by měla být obzvláště chráněna proti neoprávněné modifikaci, jiná proti zničení. S klidným svědomím lze tedy říct, že ke každým datům je z hlediska jejich ochrany nutno přistupovat zcela individuálně. Data je nutno chránit proti třem druhům nebezpečí:[63]

- *kompromitace:* chránit důvěrnost dat, tedy data před prozrazením
- *modifikace:* chránit data proti neoprávněné změně
- *zničení:* chránit data proti úmyslnému či neúmyslnému zničení

Ochranu dat lze rozdělit do několika skupin podle toho, z kterého hlediska zrovna chceme data chránit. Pro účinnou ochranu je potřeba jednotlivé přístupy vhodným způsobem kombinovat. Jako stavební kameny výsledných ochranných opatření slouží následujících pět skupin:

Ochrana fyzického přístupu k nosičům dat: je vhodné zajistit, aby se k diskům, na kterých jsou data uložena, nemohla dostat neoprávněná osoba. Zvlášť důležité je to v případě médií se zálohami.

Ochrana logického přístupu k datům: i když nikdo neoprávněný nezíská fyzický přístup k nosičům dat, může se k datům dostat. Například tím, že se přihlásí do operačního systému, který má k daným datům přístup.

Ochrana uložených dat: data uložená na disku by měla být chráněna vhodnými metodami proti neoprávněnému přečtení. Zabráníme tak situaci, kdy někdo disk přenese do jiného počítače s jiným operačním systémem a pokusí se data analyzovat.

Ochrana dat přenášených počítačovou sítí: veškeré výše popsané ochrany jsou zbytečné, pokud data přenášíme počítačovou sítí v nezabezpečené podobě.

Ochrana dat před zničením: data mohou být zničena úmyslně či neúmyslně, například vlivem přírodní katastrofy. I proti tomu se však lze snadno bránit.

Data v informačním systému lze rozdělit podle závažnosti jejich ochrany do několika skupin. Je samozřejmé, že textové soubory uživatelů nebudou chráněny stejně, jako například databáze přístupových hesel. Následující skupiny jsou seřazené vzestupně podle naléhavosti, s jakou je potřeba přistupovat k jejich ochraně:

[63] DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. 2004.

- *data uživatelů*: normální stupeň ochrany. Jejich kompromitací nebo zničením nebude narušena bezpečnost systému.
- *auditní záznamy*: zvýšený stupeň ochrany. Zničením záznamů auditu ztratíme možnost vypátrat, kdo je zodpovědný za narušení bezpečnosti systému. Platí ovšem za předpokladu, že je nějaký auditní záznam vytvářen.
- *spustitelný kód*: vysoký stupeň ochrany. Modifikací spustitelného kódu (tedy programů) může být do systému zanesena bezpečnostní díra. Právě proto musí být kód proti jakékoliv modifikaci chráněn.
- *autentizací informace*: nejvyšší stupeň ochrany. Centralizace autentizačních informací (tedy např. jmen a hesel) na jedno místo značně zesiluje motivaci útočníka. Při kompromitaci autentizačních informací může útočník v systému vystupovat s identitou jakéhokoliv uživatele. Při jejich zničení znemožní jakémukoliv uživateli přístup k systému.

4.1.1 Ochrana fyzického přístupu k nosičům dat

O ochranu přístupu k vlastním datům se stará operační systém. Zajistí, aby se k datům nedostal nikdo, kdo se k nim dostat nemá. Problém ale nastane v okamžiku, kdy je nosič dat vyjmut ze svého přirozeného prostředí a přenesen do prostředí zcela odlišeného, se zcela jinými přístupovými právy. Nosič dat může být mimo své přirozené prostřední vystaven mnohem důkladnější analýze. Dalším důvodem k zajištění fyzické bezpečnosti je možnost zničení dat. Útočník má mnohem více možností ke zničení dat, pokud má k nosičům fyzický přístup. V takovém případě mu totiž stačí mechanické nástroje. Do oblasti fyzické bezpečnosti pak spadá i ochrana proti zásahům vyšší moci, například proti živelným pohromám, neočekávaným požárům a podobně. S trochou nadsázky sem lze zařadit i ochranu proti výpadkům napájení.[64]

[64] DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. 2004.

4.2 Systém právní ochrany počítačových programů a dat

V České republice jsou počítačové programy jako moderní forma nehmotných statků právně chráněny zejména v rámci autorského zákona, obchodního zákoníku a v rámci trestního zákoníku.[65]

Ochrana dat v rámci autorského zákona. Novela autorského zákona, která byla účinná od roku 1990, zahrnovala v seznamu autorských děl také počítačové programy. V té době totiž bylo nutné přizpůsobovat se rozhodujícímu vývoji ve světě. Základní formou ochrany počítačových programů v počítačově vyspělých zemích je právě ochrana autorským právem. V současné době je v České republice daná problematika upravena zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorským zákonem).[66] Autorské právo poskytuje počítačovým programům absolutní ochranu, působící proti všem negativním vlivům. Systém autorskoprávní ochrany je podrobně rozpracován v teorii i praxi nejen u nás, ale i jinde ve světě. Podle autorského zákona je ke každému užití autorského díla nutný souhlas autora. Užitím se rozumí zejména zhotovování rozmnoženin díla, šíření, provedení překladu, úpravy a provozování díla. U počítačových programů zahrnují tyto případy realizaci rozmnoženiny nebo úpravy programu nutné pro provoz programu na počítači a pro archivní a zajišťovací účely oprávněným vlastníkem rozmnoženiny. Dále pak užití v rámci osobní potřeby, tedy nikoliv pro komerční účely, ale v omezené míře i pro účely vyučování a vzdělávací. Později byly podrobněji upraveny též případy, kdy uživatel počítačového programu není povinen získat autorovo svolení, ani poskytnout zvláštní odměnu k pořízení rozmnoženiny. Např. podle novely autorského zákona z roku 1966 došlo k velmi významnému ustanovení, které spočívá v tom, že není-li vysloveně sjednáno jinak, autorské právo k počítačovému programu vytvořeného zaměstnancem ke splnění povinnosti vyplývající z jeho pracovního poměru vykonává zaměstnavatel. Zaměstnavatel tak mohl šířit program, aniž by k tomu musel žádat o souhlas programátora, který program sestavil. Autor, jehož právo bylo porušeno, může žádat, aby bylo neoprávněné užití zakázáno, aby byly odstraněny pirátské kopie a poskytnuta mu přiměřená náhrada škody. Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi je trestným činem podle § 270 trestního zákoníku č. 40/2009 Sb.

[65] MUSIL, Stanislav. Počítačová kriminalita. Praha, 2000, s. 148.
[66] Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

Ochrana v rámci obchodního zákoníku[67]. Obchodní zákoník chrání počítačové programy v rámci obecné úpravy ochrany obchodního tajemství. Takto jsou však chráněny pouze programy, které mají nějakou hodnotu, materiální či nemateriální a nejsou běžně přístupné. Měli by být utajeny a sám podnikatel by měl jejich utajení zajistit. Uvedené podmínky velmi zužují možnosti, kdy může být efektivně uplatněna forma ochrany pouze na omezený počet případů. Ochrana proti zneužívání informací v obchodním styku je podpořena také § 255 trestního zákoníku č. 40/2009 Sb.

Ochrana v rámci ustanovení o počítačové kriminalitě. Od roku 1992 bylo přijato novelou trestního zákona zvláštní ustanovení o trestných činech poškození a zneužití záznamu na nosiči informací. Tyto činy tvoří podstatnou část počítačové kriminality. Úprav lze užít i v případech softwarového pirátství, zejména při naplnění skutkových podstat neoprávněného užití informací, neoprávněného zásahu do technického nebo programového vybavení počítače. Rovněž za tyto trestné činy jsou stanoveny sankce odnětí svobody, peněžité tresty či trest propadnutí věci. Základem systému právní ochrany počítačových programů u nás, podobně jako v jiných zemích, je ochrana autorským právem. Ochrana v rámci úpravy obchodního tajemství, případně dalších forem, týkajících se například nekalé soutěže, patentů, topografie polovodičových výrobků (čipů) apod., tvoří společně se smluvními prostředky doplňkové formy ochrany.

Licenční politika. Pro legálního výrobce softwaru jsou velmi důležité licenční smlouvy uzavírané s uživatelem, který si software regulérně zakoupí. Pokud uživatel souhlasí s podmínkami licenční smlouvy, smí softwarový produkt používat a získává zpravidla ještě další práva. Licenční smlouva nesmí být v žádném případě ve sporu s předpisy a zákony nadřazenými, tedy s ustanoveními větší právní síly. Problematika uzavírání licenčních smluv bývá nazývána licenční politikou, která může být specificky orientovaná podle zaměření, obchodní zdatnosti či jiných parametrů softwarové firmy. Ve smlouvě jsou i omezení týkající se půjčování nebo pronajímání softwaru, jeho případného dekódování nebo úprav a další omezení týkající se konkrétního produktu. Licenční smlouva také stanoví pravidla, za kterých lze pořídit záložní nebo archivní kopii produktu a obsahuje rovněž omezené záruky za software.

Odborné diskuse k problematice právních aspektů ochrany softwaru přerostly u nás v mnoha případech k obecným rozborům počítačového práva, což se projevilo v řadě připomínek k některým publikovaným pracím. V této diskusi nešlo jen o terminologické

[67] Zákon č. 513/1991 Sb., obchodní zákoník.

problémy. Byly rozebírány a podrobeny určité kritice všeobecné povahové a právní otázky nehmotných statků ve vztahu k počítačům, aspekty postavení a účinnosti novel autorského zákona, pracovněprávní poměry programátorů a jiných pracovníků kolem počítačů, trestněprávní aspekty počítačového práva, metodicko-taktické přístupy z hlediska vyšetřovatelských hledisek, otázky daňové, účetní a celní politiky, problémy obchodního práva a podnikání s počítači, aspekty ochrany informací obecně i ochrany osobních informací a soukromí občanů atp. Cílem diskuse bylo vyjasnit a precizovat situaci kolem počítačového práva i počítačové kriminality především z hlediska legislativních úprav, méně již z pohledu kriminologie. I když některé otázky zůstávají nedořešené, lze celkové aktivity v tomto směru považovat za přínosné.[68]

4.3 Softwarové pirátství a porušování autorských práv

V oblasti autorského práva je usvědčování pachatelů velmi složité. Ovšem v případě klasických pachatelů, kteří svou činnost inzerují např. v novinách, reklamních letácích či na internetu, můžou být orgány činné v trestním řízení velmi úspěšné. Typickým a jednoznačným případem byl v době nástupu vypalovacích zařízení na CD inzerát typu „vypálím jakýkoli software za 150 Kč“.[69] Jedná se o zcela jasný příklad nelegálního kopírování. Tím, že poté dojde k následnému prodeji, dochází také k porušování autorských práv. Při takovém obchodování existuje mnoho slabých míst, díky kterým je poté snadné pachatele vystopovat. Patří zde např. platby za nelegální software, které jsou uskutečňovány formou dobírky, nebo formou peněžní transakce prostřednictvím banky. V okamžiku, kdy dochází ke zveřejnění adresy, případně bankovního čísla účtu, dochází u pachatele ke ztrátě anonymity. Poté už je snadné např. prostřednictvím domovní prohlídky pachatele usvědčit. Pokud však dochází k šíření nelegálního softwaru přes internet, je policie v tomto případě, téměř bezmocná. Hlavně proto, že se jedná o decentralizované sítě, do kterých jsou napojeny miliony lidí z celého světa a není možné prošetřit tak obrovské množství uživatelů. Vždy na počátku práce orgánu činného v trestním řízení je nějaké podezření, které vyjde ze zachycení nabídky nebo poptávky po nelegálním softwaru. Většinou k tomu dochází na internetu, dříve v inzertních novinách. Motiv udání pachatele bývá různý. Může se jednat o osobu z pachatelovy blízkosti a to buď z důvodu pomsty nebo závisti, anebo se může jednat o

[68] GŘIVNA, T.; POLČÁK, R. Kyberkriminalita a právo. Praha, 2008.
[69] MATĚJKA, M. Počítačová kriminalita. Praha: Computer Press, 2002, str. 85.

čestnou osobu, která chce pouze upozornit na nekalé jednání. Prokáže-li se, že je podezření opodstatněné, musí policie nashromáždit co největší počet různých důkazů. V případě, že se opravdu jedná o pachatele této trestné činnosti, může provést domovní prohlídku, nebo zajistit počítač podezřelého. Právě v osobních počítačích se většinou nacházejí přímé důkazní materiály, které pomohou pachatele jednoznačně usvědčit. Někdy se ovšem stává, že pachatel stihne ještě před příchodem policie, svá data, která by ho mohla usvědčit, vymazat. V tom případě je práce orgánu činného v trestním řízení značně zkomplikována. V dnešní době však vyšetřovatelé disponují prostředky, které dokážou poměrně snadno i smazaný obsah určitým způsobem obnovit. Pachatel ale nemusí v žádném případě policii potvrzovat legálnost používaného softwaru, stejně tak není povinen prozrazovat hesla do systému, případně kódy k zašifrovaným souborům. Tato skutečnost nesmí být brána jako přitěžující okolnost, neboť důkazní břemeno nese pouze orgán činný v trestním řízení. Naopak však, pokud pachatel tato hesla sdělí a s policií spolupracuje, lze při výměře trestu k tomuto přihlížet jako na polehčující okolnost.[70]

Z výše uvedených skutečností vyplývá, že metodika odhalování a dokazování počítačové kriminality a trestných činů s ní souvisejících, je v určitých stádiích odlišná od ostatní běžně se vyskytující kriminality materiální. Je také patrné, že s podobnými postupy se nelze setkat jinde, než právě u tohoto druhu deliktů. Vyšetřování počítačové kriminality však závisí také na modernizování prostředků běžných pro vyšetřování a je náročné na odbornost a vzdělání lidí. Jedině s takovými prostředky je možné držet krok s pachateli, případně být o krok napřed ať už ve fázi odhalování, nebo následnému dokazování této trestné činnosti.

4.3.1 Nelegální software

V dnešní době existuje nespočetné množství softwaru, který je určen pro různá použití. Existuje ve formě komerčních, či nekomerčních programů a je vázán velkým množstvím typů licenčních smluv. Což je také důvod, který může vést i naprosté laiky k porušování autorských práv. Důležitým faktem však zůstává, že z větší části jsou autorská práva porušovaná úmyslně a většinou za účelem neoprávněného zisku. Tím dochází ke snižování dostupnosti kvalitního softwaru, neboť dodavatelé jsou nuceni takto ušlé náklady zakalkulovat do své ceny. Porušování práva duševního vlastnictví, při kterém je software používán nebo distribuován bez platné licence, nebo v rozporu s tou licencí, lze nazvat jako

[70] MATĚJKA, M. Počítačová kriminalita. Praha: Computer Press, 2002, str. 85

softwarové pirátství. Používání, distribuci a další nakládání se softwarem upravuje autorský zákon a nákup či prodej se řídí zákoníkem občanským a obchodním.[71] V souvislosti s počítačovým pirátstvím bývá nejen v médiích uváděno, že za porušování autorského práva hrozí trestněprávní postih i běžným uživatelům nelegálního softwaru.[72]

Nelegálním používáním softwaru, hrozí tři typy sankcí:

- sankce občanskoprávní,
- sankce veřejnoprávní, a to:
    - postih za přestupek na úseku kultury,
    - postih za trestný čin porušování autorského práva, práv souvisejících s právem autorských a práv k databázi.

Jak přestupky, tak trestné činy jsou v českém právu určeny kombinací formálního a materiálního znaku, tedy znaků příslušných deliktů uvedených v ustanoveních trestního zákoníku či přestupkového zákona a stupněm nebezpečnosti jednání pro společnost. V případě, že za stejný skutek připadá v úvahu jak odpovědnost za přestupek, tak odpovědnost za trestný čin, je třeba zkoumat formulaci příslušných skutkových podstat uvedenou v trestním zákoníku a přestupkovém zákoně a v případě, že z pouhého rozdílu formálních znaků nelze určit, zda je dané jednání trestným činem či přestupkem, je třeba rozhodnout, zda je v daném případě určitý skutek postižitelný jako přestupek či jako trestný čin podle stupně nebezpečnosti daného jednání pro společnost.[73] U porušování autorských práv, literatura[74] většinou uvádí právě tyto okolnosti pro posouzení společenské nebezpečnosti daného jednání:

- Význam chráněného zájmu, který byl činem dotčen. Zde je třeba posoudit význam konkrétního autorského práva, které je porušeno.
- Způsob provedení činu. Tato okolnost nebude zřejmě v případě porušení autorského práva příliš praktická, obecně se jedná např. o spáchání činu se zbraní, veřejně, zvláště zavrženíhodným způsobem apod. Význam ale může mít například to, že pachatel, který autorské právo porušil, tak činil ve skupině či za pomoci dalších uživatelů, ani

[71] Co je softwarové pirátství? Dostupné z www.bsa.org.
[72] MATĚJKA, M. Postih porušování autorského práva běžnými uživateli software aneb je nevýdělečné používání nelegálního software pro osobní potřebu opravdu trestným činem? 2003. Dostupné z http://www.itpravo.cz/index.shtml?x=147455#2.
[73] NOVOTNÝ, O. Trestní právo hmotné - I. obecná část. 1997, str. 61.
[74] NOVOTNÝ, O. Trestní právo hmotné - I. obecná část, 1997.

tato skutečnost ovšem není pro domácí nevýdělečné porušování autorského práva typická.

- Trvání a intenzita činu. Zde půjde především o to, jak dlouho pachatel autorské právo porušoval, jak často nelegální počítačové programy používal apod.
- Následky. Zde půjde opět o úvahu nad povahou a dopady porušení autorského práva v daném případě, zejména vzhledem k tomu, co bylo výše řečeno o druhovém a individuálním objektu porušování autorského práva.
- Rozsah škody. Výše způsobené škody není znakem skutkové podstaty ani trestného činu porušování autorského práva ani přestupku na úseku kultury, přesto může mít v konkrétním případě význam pro stanovení společenské nebezpečnosti činu. Problematické je ovšem určení výše škody. Poškozené subjekty preferují vyčíslení formou ušlého zisku, tedy například používá-li někdo nelegálně software, jehož originální kopie stojí běžně 5000 Kč, vyčíslují škodu právě v této výši. I bez shody na metodě vyčíslení škody lze však říci, že větší počet nainstalovaných nelegálních programů znamená větší výši škody (ať již jakkoli vyčíslené) a tedy i vyšší společenskou nebezpečnost pachatelova jednání v konkrétním případě.
- Okolnosti, za kterých byl čin spáchán. Zde může jít o různé vlivy související s místem a časem spáchání činu. Uvádí se[75], že vyšší stupeň společenské nebezpečnosti mají činy, jež se v určité době na určitém místě rozmáhají. V souvislosti s četností porušování autorského práva drobnými uživateli je ale na místě otázka, kdy jde ještě o rozmach kriminality, která je stále i přes tento její rozmach za kriminalitu považována a kdy rozšíření určitého jednání, doposud trestněprávně postihovaného, naopak znamená spíše společenskou tendenci k jeho dekriminalizaci a tedy i podstatné snížení stupně společenské nebezpečnosti takového jednání.
- Osoba pachatele. Na místě je zde zkoumat osobnost a chování pachatele vzhledem ke spáchanému deliktu. Jde o osobní a profesní postavení pachatele, jeho chování před činem i po něm, postoj pachatele k trestnému činu apod.
- Míra zavinění. Zde obecně platí, že přímý úmysl vykazuje vyšší stupeň společenské nebezpečnosti než nepřímý, totéž lze ale říci o nedbalosti vědomé a nevědomé. Dále může mít význam například to, zda se jednalo o čin uvážený, dopředu připravovaný, nebo čin provedený náhle, bez předchozí úvahy.

[75] Zákon č. 40/2009 Sb., trestní zákoník.

- Pohnutka. Zde půjde především o to, z jakého důvodu pachatel delikt porušení autorského práva spáchal. Může jít např. o prostou neochotu platit za legální softwarové produkty, snahu způsobit škodu poškozeným subjektům a v neposlední řadě třeba i o určitý druh zábavy.

V roce 2010 provedla protipirátská organizace BSA[76] studii věnovanou softwarovému pirátství.[77] Ze studie vyplývá, že softwarové odvětví bitvu s piráty dlouhodobě vyhrává. Míra pirátství klesla za poslední dva roky navzdory globální hospodářské krizi o procentní bod. Průzkum sledoval užívání nelegálních počítačových programů ve více než stovce zemí světa. Počet instalací nelegálního softwaru v tuzemských osobních počítačích klesl meziročně o 1 %. Podle Jana Hlaváče, tiskového mluvčí BSA, dosahuje míra pirátství 37 %. V důsledku toho přišli výrobci softwaru v České republice o tržby v hodnotě 3,6 miliardy korun. Odhlédne-li se od trestněprávních rizik, tak nelegální software často obsahuje škodlivé počítačové kódy, které mohou ohrozit bezpečnost dat uživatelů. K růstu míry pirátství naopak přispívá rychlý růst trhu s výpočetní technikou a větší užívání starších počítačů, v nichž výskyt nelegálního softwaru převládá. Svou roli hraje i čím dál větší rafinovanost pirátů kybernetických zločinů. Míru pirátství snižují mimo jiné také legalizační programy, osvětové kampaně vládních úřadů i softwarových firem, kroky orgánů činných v trestním řízení a také změny technologií, jako jsou stále rozšířenější nástroje pro správu digitálních práv.

4.4 Porušování předpisů o ochraně osobních údajů

Základním pramenem pro právní úpravu osobních údajů je zákon č. 2/1993 Sb., Listina základních práv a svobod jako součást ústavního pořádku České republiky, ve kterém je zakotveno i právo na ochranu osobních údajů. V čl. 7 Listina zakotvuje právo na nedotknutelnost osoby a jejího soukromí, v čl. 10 odst. 3 upravuje právo každého na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě a v čl. 13 stanoví, že nikdo nesmí porušit listovní tajemství ani tajemství jiných písemností a záznamů, ať již uchovávaných v soukromí, nebo zasílaných poštou anebo jiným

[76] Business Software Alliance je mezinárodní protipirátská organizace, která zastupuje softwarové firmy z celého světa.
[77] Business Software Alliance. Pirátského softwaru v Česku opět ubylo, nelegálně se ho užívá 37 %. 2010. Dostupné z http://portal.bsa.org/globalpiracy2009/pr/pr_czech.pdf.

způsobem, s výjimkou případů a způsobem, které stanoví zákon. Stejně tak se zaručuje tajemství zpráv podávaných telefonem, telegrafem nebo jiným podobným zařízením.[78]

Ochrana osobních údajů je v České republice regulována zákonem č. 101/2001 Sb., o ochraně osobních údajů a změně některých zákonů a dalšími právními předpisy.[79] Tento zákon vymezuje působnost pojmů, práva a povinnosti při zpracování osobních údajů, povinnosti osob, likvidaci osobních údajů, ochranu práv subjektů, nápravu nemajetkové újmy či škody a předávání osobních údajů do jiných států. Na základě zákona dochází ke zřízení nezávislého Úřadu pro ochranu osobních údajů, k úpravě jeho postavení, působnosti, organizace, činnosti kontrol či sankciování. Úřad pro ochranu osobních údajů má kompetence správního úřadu.

Vlivem mnoha technologických či vývojových změn byl zákon o ochraně osobních údajů několikrát novelizován. Tento zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci a fyzické a právnické osoby. Zákon se nevztahuje na zpracování osobních údajů fyzických osob, které používají údaje pouze pro vlastní potřebu. Jedná se především o záležitosti rodinného a soukromého života. Zpracování osobních údajů pro statistické účely a archivnictví stanoví zvláštní zákony. Tzn., že pokud zákon o státní statistické službě nebo zákon o archivnictví a spisové službě obsahují zvláštní úpravu, mají poté přednost před úpravou obecnou.

„Osobním údajem se rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“[80] Základním kritériem pro posouzení, zda se jedná o osobní údaj či nikoliv, je okolnost zjištění identity subjektu údajů. Vychází se ze skutečnosti, zda správce může vytvořit přímou vazbu mezi údajem a fyzickou osobou.

Zákon definuje další důležité pojmy ve vztahu k osobním údajům:[81]

- *anonymní údaje*: jsou ty, které v původním tvaru nebo po provedeném zpracování nelze vztáhnout k určitému subjektu údajů (např. osobní údaje zařazené do velkých statistických souborů, které jsou zbaveny jména, příjmení a rodného čísla).

[78] Listina základních práv a svobod. Dostupné z http://www.psp.cz/docs/laws/listina.html.
[79] Zákon č. 101/2001 Sb., o ochraně osobních údajů.
[80] Zákon č. 101/2000 Sb., o ochraně osobních údajů.
[81] DOLEČEK, M. Ochrana osobních údajů. 2010. Dostupné z http://www.businessinfo.cz/cz/clanek/orientace-v-pravnich-ukonech/ochrana-osobnich-udaju-opu/1000818/51144/#b1.

- *zveřejněný údaj*: jímž se rozumí ten, který je zpřístupněný hromadným sdělovacím prostředkem, jiným veřejným sdělením (např. na schůzi, v odborné literatuře, na plakátu) nebo je součástí veřejného seznamu (může jít jak o úřední seznam, tak o seznam vydávaný soukromým subjektem pro komerční účely). Zveřejnění se ovšem může stát i jiným způsobem.
- *správce*: jímž je každý subjekt, který určuje účel a prostředky zpracování, provádí zpracování a odpovídá za něj. Nezbytným znakem správce však není zpracování osobních údajů vzhledem k tomu, že touto činností může být zvláštním zákonem zmocněn, nebo správcem na základě smlouvy pověřen zpracovatel (např. každý advokát je tedy správcem osobních údajů, který současně osobní údaje zpracovává, protože s ohledem na jeho činnost zřejmě nepřichází v úvahu, aby zpracováním někoho pověřil).

4.4.1 Práva a povinnosti správců a zpracovatelů osobních údajů

Zákon rozlišuje osoby, které zpracovávají osobní údaje dalších lidí a také osoby, jejichž osobní údaje správci a zpracovatelé zpracovávají. Správcům a zpracovatelům jsou ze zákona určeny především povinnosti, zatímco subjektům jsou dána práva. Na ochranu práv subjektů údajů a kontrole plnění povinností správce a zpracovatele osobních údajů byl zřízen Úřad na ochranu osobních údajů. Za neplnění povinností hrozí sankce. Plnění povinností správci a zpracovateli předpokládá tyto povinnosti znát a vědět, jak je realizovat. K výkladu zákona i k objasnění jednotlivých povinností a k praktickým prováděním ochrany osobních údajů lze využít různé nástroje, např. právní předpisy[82] a odbornou literaturu.[83]

Každý správce a zpracovatel osobních údajů musí dbát na to, aby žádný subjekt, jehož osobní údaje jsou zpracovávány, neutrpěl újmu na svých právech. V této situaci jde především o právo na zachování lidské důstojnosti a na ochranu před neoprávněným zasahováním do osobního a soukromého života. V tomto smyslu je nutné vykládat všechna ustanovení daného zákona. Pokud dojde k porušení daných povinností, Úřad pro ochranu osobních údajů uloží správci či zpracovateli osobních údajů pokutu. Jejich odpovědnost je postavena na tzv. objektivním principu s možností liberace. Což znamená, že již není zkoumána skutečnost, zda vůbec došlo k porušení povinností jejich vlastním zaviněním, ale jde především o to, že vůbec k porušení daného zákona došlo. Jiná situace však nastává, pokud jsou správci a zpracovatelé

[82] Právní předpisy. Dostupné z http://www.uoou.cz/uoou.aspx?menu=4.
[83] Ochrana osobních údajů. Dostupné z http://www.oou.cz/.

schopni prokázat, že i přes veškerou snahu a úsilí z jejich strany, nebylo v žádném případě možné takovému provinění zabránit. Pokud tedy dojde ke zneužití osobních údajů vinou předchozího teroristického útoku, nebude možné vůči správci či zpracovateli vyvodit důsledky. Jestliže však např. banka nezajistí svou databázi klientů proti zneužití, bude za to nést zodpovědnost.[84]

V § 180 trestního zákoníku č. 40/2009 Sb., ve znění pozdějších předpisů, je vymezena skutková podstata trestného činu neoprávněného nakládání s osobními údaji. Trestného činu se dopustí ten, kdo, byť i z nedbalosti, neoprávněně sdělí, zpřístupní, jinak zpracovává nebo si přisvojí osobní údaje o jiném, shromážděné v souvislosti s výkonem veřejné moci a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají. Stejného trestného činu se dopustí i ten, kdo byť i z nedbalosti, poruší státem uloženou nebo uznanou povinnost mlčenlivosti tím, že neoprávněně zveřejní, sdělí nebo zpřístupní třetí osobě osobní údaje získané v souvislosti s výkonem svého povolání, zaměstnání nebo funkce a způsobí tím vážnou újmu na právech nebo oprávněných zájmech osoby, jíž se osobní údaje týkají. Objektem tohoto trestného činu je zájem státu, resp. společnosti na dodržování zákonem stanovené povinnosti mlčenlivosti. Objektivní stránku naplňuje jednání spočívající v současném splnění několika výše uvedených podmínek.[85]

Pokud dojde k porušení zákona, tedy k případnému zneužití osobních údajů, je dle zákona ukládána správcům a zpracovatelům osobních údajů pokuta. Sankce jsou vyměřovány podle závažnosti provinění a jsou ukládány Úřadem pro ochranu osobních údajů. Úřad mimo jiné řeší porušení povinností. Zaplacené pokuty jsou příjmem do státního rozpočtu a s vymáháním Úřadu pomáhá finanční orgán. Veškeré přestupky jsou projednávány dle zákona č. 200/1990 Sb., o přestupcích, ve znění pozdějších předpisů.

Sankce jsou upraveny v Hlavě VII. zákona o ochraně osobních údajů. Jsou zde rozlišeny sankce za přestupky a jiné správní delikty.

Za *přestupek* je považováno např. porušení mlčenlivosti u osoby, která je v pracovním poměru se správcem či zpracovatelem osobních údajů. Další přestupky jsou specifikovány v § 44 odst. 2 a 3.[86] Fyzická osoba se jako správce nebo zpracovatel dopustí přestupku tím, že při zpracování osobních údajů např. nestanoví účel, prostředky nebo způsob zpracování, nebo stanoveným účelem zpracování poruší povinnost, nebo překročí oprávnění vyplývající ze zvláštního zákona, zpracovává nepřesné osobní údaje, shromažďuje nebo zpracovává osobní

[84] DOLEČEK, M. Ochrana osobních údajů. 2010. Dostupné z http://www.businessinfo.cz/cz/clanek/orientace-v-pravnich-ukonech/ochrana-osobnich-udaju-opu/1000818/51144/#b1.
[85] Zákon č. 40/2009 Sb., trestní zákoník.
[86] Zákon č. 101/2000 Sb., o ochraně osobních údajů.

údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu, uchovává osobní údaje po dobu delší než nezbytnou k účelu zpracování, zpracovává osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně, neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem, odmítne subjektu údajů poskytnout požadované informace, nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů a nebo nesplní oznamovací povinnost podle tohoto zákona.

Přestupkem je podle § 44a rovněž zveřejnění osobních údajů i přes zákaz stanovený zvláštním právním předpisem. Zákon zde má na mysli zejména ustanovení zákona č. 141/1961 Sb., trestního řádu ve znění novely - tzv. „náhubkového zákona". Trestní řád zakazuje zveřejnění:[87]

- informace umožňující zjištění totožnosti poškozeného, který je buď mladší 18 let, nebo vůči němuž byl spáchán některý z vyjmenovaných trestných činů (trestné činy proti životu a zdraví, svobodě a lidské důstojnosti, proti rodině a mládeži, trestný čin kuplířství a šíření pornografie),
- jakéhokoliv záznamu z průběhu hlavního líčení nebo veřejného zasedání soudu, pokud by umožnily zjištění totožnosti dle předchozího odstavce,
- pravomocného rozsudku s údaji umožňujícími identifikaci (tedy takové údaje je třeba při případném zveřejnění začernit),
- informací o nařízení či provedení odposlechu a záznamu telekomunikačního provozu stejně jako informací z odposlechu získaných.

Správního deliktu se dopustí fyzická nebo právnická osoba, která je správcem či zpracovatelem osobních údajů a při vykonávání své činnosti nestanoví účel, prostředky nebo způsob zpracování, nebo poruší povinnost a překročí oprávnění vyplývající ze zvláštního zákona, zpracovává nepřesné osobní údaje, shromažďuje nebo zpracovává osobní údaje v rozsahu nebo způsobem, který neodpovídá stanovenému účelu uchovává osobní údaje po dobu delší než nezbytnou k účelu zpracování, zpracovává osobní údaje bez souhlasu subjektu údajů mimo případy uvedené v zákoně, neposkytne subjektu údajů informace v rozsahu nebo zákonem stanoveným způsobem, odmítne subjektu údajů poskytnout požadované informace, nepřijme nebo neprovede opatření pro zajištění bezpečnosti zpracování osobních údajů, nesplní oznamovací povinnost podle tohoto zákona.

[87] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád).

Správním deliktem je podle § 45a rovněž zveřejnění osobních údajů i přes zákaz stanovený zvláštním právním předpisem. Zákon zde má na mysli zejména ustanovení zákona č. 141/1961 Sb., trestního řádu ve znění novely - tzv. „náhubkového zákona."

Při rozhodování o sankcích přihlíží Úřad pro ochranu osobních údajů především k závažnosti, povaze, míry zavinění, způsobu jednání, doby trvání a následku protiprávního jednání. Do 1 roku smí Úřad uložit pokutu a to ode dne, kdy bylo zjištěno porušení zákona příslušným orgánem, nejdéle však do 3 let ode dne, kdy došlo k porušení povinnosti.[88]

[88] DOLEČEK, M. Ochrana osobních údajů. 2010. Dostupné z http://www.businessinfo.cz/cz/clanek/orientace-v-pravnich-ukonech/ochrana-osobnich-udaju-opu/1000818/51144/#b1.

5 Závěr

V současné době je počítačová kriminalita velice diskutovaným tématem a zasluhuje si velkou dávku pozornosti ze strany laické i odborné veřejnosti, ale také ze strany orgánů činných v trestním řízení. V mé diplomové práci jsem se snažila poukázat na její nejdůležitější projevy, ale také na její všeobecný dopad na společnost. Kladla jsem důraz na ucelenost, systematičnost a pojmovou rozsáhlost tohoto druhu trestné činnosti.

V úvodní části práce jsem se věnovala teoretickému výkladu obecné terminologie pojmu „počítačová kriminalita“ z různých hledisek, přičemž důraz byl kladen na specifikaci definovanou v *Úmluvě o počítačové kriminalitě* vydanou *Radou Evropy*. Za velmi důležité jsem považovala seznámení čtenářů s historickým vývojem tohoto druhu kriminality. Pro úplné pochopení důvodů vzniku počítačových hrozeb bylo nezbytně nutné uvést vzájemné souvislosti s vývojem výpočetní techniky a informačních technologií. V této části jsem se také zaměřila na preventivní opatření, jakožto velmi důležitý prvek v boji s počítačovou kriminalitou. Spolu s výše zmíněnými skutečnostmi jsem uvedla také charakteristiku osobnosti pachatele této trestné činnosti, jeho psychologický profil a motivaci k protiprávnímu jednání. Za velmi důležité jsem považovala také uvedení faktu, že tito pachatelé patří ke vzdělanější vrstvě společnosti.

Ve stěžejní a zároveň nejrozsáhlejší části mé diplomové práce jsem do tří podkapitol rozčlenila hlavní dopady počítačové kriminality na společnost a to jak z právního tak ekonomického hlediska. Tyto důsledky jsem klasifikovala také podle dopadu konkrétních skutků. Pro nastínění situace v České republice jsem do této části zahrnula také příslušné zákony a zaměřila jsem se na trestněprávní úpravu hrozeb souvisejících s počítačovými delikty. Všechna protiprávní jednání uvedená v této části byla kvalifikována dle skutkových podstat trestných činů, které je naplňují. Jako nezbytné pro srovnání situace u nás a v zahraničí jsem považovala uvedení konkrétních trestných činů a jejich rozdílných důsledků. Nejrozsáhlejší forma tohoto druhu trestné činnosti je kyberkriminalita na internetu a kyberterorismus, jehož součástí je také kyberšikana, proto jsem se na tuto problematiku velmi podrobně zaměřila. Snahou bylo poukázat na to, že i nová protiprávní jednání, související právě s počítačovou kriminalitou, jsou postižitelná současnou úpravou trestního zákoníku, ale to jen v případě, že je odhalen konkrétní pachatel a jsou nalezeny potřebné důkazy usvědčující jeho protiprávní jednání. Z toho vyplývá, že hlavní problém v dokazování informačních deliktů nespočívá až tak v nedostatečné právní úpravě, nýbrž ve velmi náročném procesu

odhalování pachatele. Z důvodu pojmové náročnosti problematiky specifických jednání, která se uskutečňují prostřednictvím počítače, jako nástroje, jsem byla nucena v některých částech popis jednotlivých činů zjednodušit tak, abych se vyhnula náročné a odborné terminologii, což by bylo nad rámec diplomové práce.

Závěrečná část práce je věnována ochraně dat. Jedná se o velmi důležitou součást preventivních opatření vztahujících se k počítačové kriminalitě. Zaměřila jsem se především na problematiku porušování autorských práv a její trestněprávní úpravu. Jako nezbytnou součást kapitoly o ochraně dat jsem považovala také problematiku zabývající se porušování předpisů o ochraně osobních údajů.

Diplomová práce by také nemohla být kompletní bez zmínky o organizacích bojujících s touto problematikou „digitálního věku“ a to jak na území České republiky, tak v zahraničí. Z výše zmíněného vyplývá, že většina z protiprávních jednání překračují hranice státu, ve kterém k nim došlo a tím i jejich negativní účinek. Z tohoto důvodu je tedy velmi důležitá mezinárodní spolupráce represivních orgánů, ale také nevládních mezinárodních organizací, které jsou na boj s počítačovou kriminalitou zaměřeny.

Hlavním cílem mé diplomové práce bylo poukázat na aktuální, zajímavé a nejznámější projevy počítačové kriminality a specifikovat důsledky, které páchání této trestné činnosti vznikají. Čtenář by měl získat ucelený přehled o této oblasti, samozřejmě však v omezeném rozsahu, neboť veškerá protiprávní jednání činěná za pomocí informačních technologií by mohla být námětem pro vydání rozsáhlé publikace.

Věřím, že jsem svou diplomovou prací osvětlila alespoň z malé části tuto velmi zajímavou problematiku a umožnila tak jejímu čtenáři seznámení s nejdůležitějšími aspekty počítačové kriminality.

Seznam použité literatury

Tištěné zdroje

BÍMOVÁ, A. Počítačová kriminalita a naše doba. 1. Vyd. Praha: IDG Czech, 1993. 137 s. ISBN 80-900872-2-1.

DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. 1. Vyd. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

DYTRT, Z.; MIKULECKÝ, P.; NEJEZCHLEBA, M.; PRILLWITZ, G,; ROUDNÝ, R. *Etika podnikání a veřejné správy: Informační společnost – etická výzva pro 21. století.* 1. Vyd. Praha: VUSTE ENVIS, 1999, ISBN 80-902356-5-4.

GŘIVNA, T.; POLČÁK, R. Kyberkriminalita a právo. 1. Vyd. Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.

MATĚJKA, M. Počítačová kriminalita. 1. Vyd. Praha: Computer Press, 2002. 106 s. ISBN 80-7226-419-2.

MUSIL, S. Počítačová kriminalita: Nástin problematiky. 1. Vyd. Praha: Institut pro kriminologii a sociální prevenci, 2000. 281 s. ISBN 80-86008-80-0.

NOVOTNÝ, O.; DOLENSKÝ, A.; JELÍNEK, J.; VANDUCHOVÁ, M., *Trestní právo hmotné, I. Obecná část.* 3. Vyd. Praha: Codex, 1997. ISBN 80-85963-24-8.

SMEJKAL, V. Počítačové právo. 1. Vyd. Praha: C.H. Beck, 1995. 264 s. ISBN 80-7179-009-5.

Tištěná periodika

SVETLÍK, M. *Informační bezpečnost: část 1-4.* Softwarové noviny. 2002, č. 2-5.

Elektronické zdroje

AMBROŽ, J. Jak silná je naše „softwarová policie“ [online]? [cit. 2005-05-24]. Dostupný z WWW: <http://www.lupa.cz/clanky/jak-silna-je-nase-softwarova-policie/>.

Business Software Alliance [online]. [cit. 2011-04-25]. Dostupný z WWW: <www.bsa.org>.

Business Software Alliance. Pirátského softwaru v Česku opět ubylo, nelegálně se ho užívá 37 % *News release* [online]. 2009. [cit. 2010-05-11]. Dostupný z WWW: <http://portal.bsa.org/globalpiracy2009/pr/pr_czech.pdf>.

Co je softwarové pirátství [online]? 2011. Dostupný z WWW: <www.bsa.org>.

DENNING, D. E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy [online]. 2010. Dostupný z WWW: <http://www.nautilus.org/infopolicy/ workshop/papers/denning.html>.

DOLEČEK, M. Ochrana osobních údajů [online]. [cit. 2010-06-18]. Dostupný z WWW: <http://www.businessinfo.cz/cz/clanek/orientace-v-pravnich-ukonech/ochrana-osobnich-udaju-opu/1000818/51144/#b1>.

IFPI [online]. [2011-04-25]. Dostupný z WWW: <www.ifpicr.cz>.

JANOUŠEK, M. Kyberterorismus: terorismus informační společnosti. Obrana a strategie [online]. 2/2006. Dostupný z WWW: <http://www.army.cz/mo/obrana_a_strategie/2-2006cz/janousek.pdf>.

JIROVSKÝ, V.; HNÍK, V.; KRULÍK, O. Kybernetické hrozby: výzva pro moderní společnost [online]. 2008. Dostupný z WWW: <http://aplikace.mvcr.cz/archiv2008/bezpecnost/informacni/kyberneticke_hrozby.pdf>.

KŘESŤANOVÁ, L. Kyberšikana, aneb Nikdy nevíš kdo je na druhé straně. *Nástrahy doby* [online]. 4-5 2009. [cit. 2009-05-26]. Dostupný z WWW: <http://ruce.cz/clanky/595-kybersikana-aneb-nikdy-nevis-kdo-je-na-druhe-strane>.

KŘÍŽ, L. X-vize budoucí bezpečnosti [online]. 2006. Dostupný z WWW: <http://www.computerworld.cz/cw.nsf/ID/B7AE352FC15C49A9C12570E9006B5837?OpenDocument&cast=1>.

KUCHAŘÍK, K. Činnost policie ČR ve vztahu k informační kriminalitě [online]. [cit. 2011-04-25]. Dostupný z WWW: <http://i.iinfo.cz/Karel_Kucharik_Cinnost_Policie_CR_ve_vztahu_k_informacni_kriminalite-123572804005458.ppt>.

KUCHAŘÍK, K. Kriminalita na internetu [online]. 2010. Dostupný z WWW: <http://info.muni.cz/txt/1009/19.html>.

Kyberprostor. *Wikipedia – the Free Encyclopedia* [online]. 2011. Dostupný z WWW: <http://en.wikipedia.org/wiki/Cyberspace>.

Listina základních práv a svobod [online]. 2011. Dostupný z WWW: <http://www.psp.cz/docs/laws/listina.html>.

MATĚJKA, M. Postih porušování autorského práva běžnými uživateli software aneb je nevýdělečné používání nelegálního software pro osobní potřebu opravdu trestným činem? *Rubrika: Odpovědnost a delikty, Autorská a průmyslová práva* [online]. 2011. [cit. 2003-10-14]. Dostupný z WWW: <http://www.itpravo.cz/index.shtml?x=147455#2>.

Ministerstvo vnitra České republiky. Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky v roce 2010. Praha. [cit. 2011-04-25]. Dostupný z WWW: <www.mvcr.cz/soubor/zprava-komplet-2009-pdf.aspx>.

MOUNTAIN VIEW. Nenápadná epidemie: počítačová kriminalita postihuje více než dvě třetiny uživatelů Internetu. *Tisková zpráva* [online]. [cit. 2010-09-08] Dostupné z WWW: <http://www.symantec.com/cs/cz/about/news/release/article.jsp?prid=20100908_02>.

MUSIL, S. Počítačová kriminalita. *Institut pro kriminologii a sociální prevenci* [online]. 2000, Praha. [2011-04-25]. ISBN 80-86008-80-0. Dostupný z WWW: <http://www.ok.cz/iksp/docs/256.pdf>.

PAUKERTOVÁ, Veronika. Elektronická informační kriminalita. *Ikaros* [online]. 2006, roč. 10, č. 8 [cit. 2011-04-25]. ISSN 1212-5075. Dostupný na WWW: <http://www.ikaros.cz/node/3554>.

POLICIE ČR. Šikana [online]. 2010. Dostupný z WWW: <http://www.policie.cz/clanek/preventivni-informace-sikana.aspx>.

POŽÁR, J. Některé trendy informační války, počítačové kriminality a kyberterorismu [online]. 2005. Dostupný z WWW: <http://www.svses.cz/skola/akce/konf/bezp05/texty/pozar.pdf>.

STERLING, B. Zátah na hackery - chaos a nepořádek v elektronickém pohraničí. *"The Hacker Crackdown" - časopis Natura* [online]. 12/1995 - 07/1996. 2011. Dostupný z WWW: < http://knihovnicka.mysteria.cz/zatah.pdf>.

Šikana a kyberšikana [online]. 2011. Dostupné z WWW: <http://proti-sikane.saferinternet.cz/sikana-a-kybersikana>.

TOLAR, O. Policie je krátká na weby popírající holocaust [online]. [cit. 2006-02-22]. Dostupný z WWW: <http://zpravy.idnes.cz/ krimi.asp?r=krimi&c=A060222_114752_krimi_ton>.

Úmluva o počítačové kriminalitě [online]. Budapešť. [cit. 2001-11-23]. Dostupný z WWW: <http://translate.google.cz/translate?hl=cs&langpair=en|cs&u=http://en.wikipedia.org/wiki/Convention_on_Cybercrime>.

Virtuální ponižování aneb kyberšikana [online]. [cit. 2010-02-18]. Dostupné z WWW: <http://www.inflow.cz/virtualni-ponizovani-aneb-kybersikana>.

Právní předpisy

Ochrana osobních údajů [online]. 2011. Dostupný z WWW: < http://www.oou.cz/>.

Právní předpisy [online]. Dostupný z WWW: <http://www.uoou.cz/uoou.aspx?menu=4>.

Ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod, ve znění pozdějších předpisů.

Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

Zákon č. 40/2009 Sb., trestní zákoník.

Zákon č. 101/2000 Sb., o ochraně osobních údajů.

Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád).

Zákon č. 513/1991 Sb., obchodní zákoník.

Zákon č. 40/1964 Sb., občanský zákoník.

Zákon č. 40/1995 Sb., o regulaci reklamy.

Zákon č. 127/2005 Sb. o elektronických komunikacích.

Seznam zkratek

BSA – Business Software Alliance

EU – Evropská Unie

IFPI – Mezinárodní federace fonografického průmyslu

IT – Informační technologie

WWW – World Wide Web (označení pro celosvětovou síť)

TrZ – Zákon č. 40/2009 Sb., Trestní zákoník, ve znění pozdějších předpisů

BBS – Bulletin Board System (předchůdce dnešního Internetu)

ÚOKFK – Útvar odhalování korupce a finanční kriminality

PČR – Policie České republiky

IBM - International Business Machines Corporation

Prohlášení o využití výsledků diplomové práce

Prohlašuji, že
- jsem byl(a) seznámen(a) s tím, že na mou diplomovou (bakalářskou) práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;
- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou (bakalářskou) práci užít (§ 35 odst. 3);
- souhlasím s tím, že diplomová (bakalářská) práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové (bakalářské) práce. Souhlasím s tím, že bibliografické údaje o diplomové (bakalářské) práci budou zveřejněny v informačním systému VŠB-TUO;
- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;
- bylo sjednáno, že užít své dílo, diplomovou (bakalářskou) práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 29. dubna 2011

……
jméno a příjmení studenta

Adresa trvalého pobytu studenta:

Svatopluka Čecha 546/4

73601 Havířov – Město